offerings

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.
Forwarding and Address Correction Requested

SECOND CLASS POSTAGE
Permit PAID at
East Setauket, N.Y.
11733

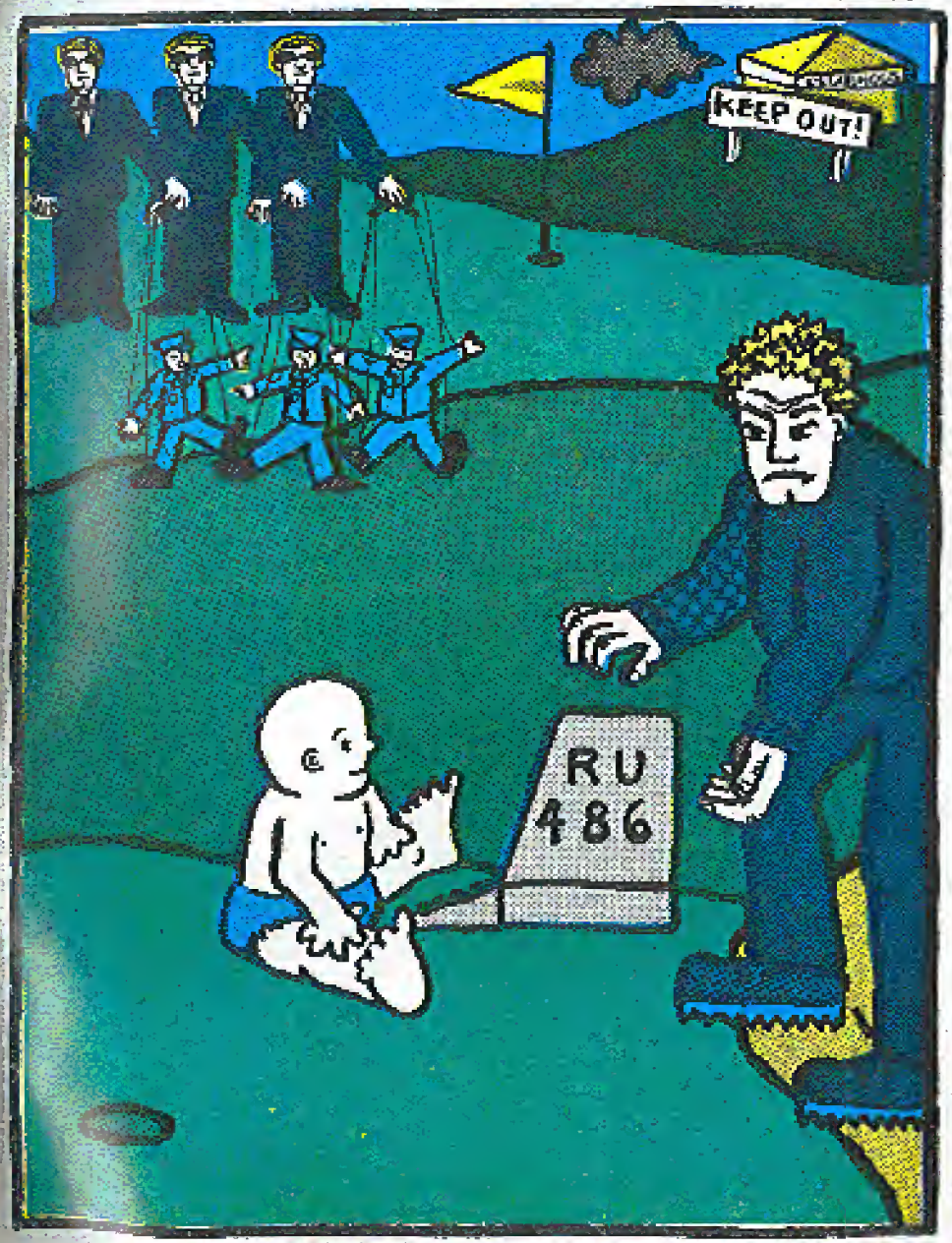
ISSN 0749-3851

2600

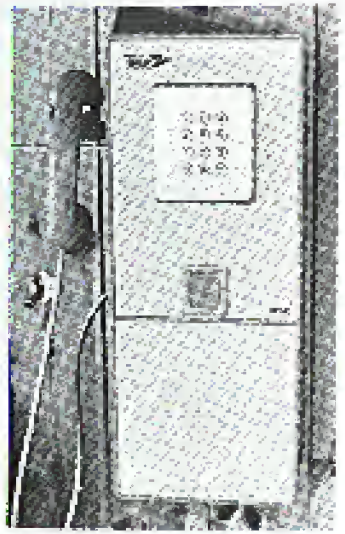
NATIONAL TECHNICAL MEANS

The Hacker Quarterly

VOLUME NINE, NUMBER FOUR
WINTER 1992-93



NORWEGIAN PAYPHONES



Three different types of Norwegian payphones. Note the strange positioning of the numbers on the keypad. The mobile payphone was spotted on a tour bus.

Photos by JR of New York.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. NORTH KOREAN PAYPHONES WANTED!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada -- $21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988, 1989, 1990, 1991 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us

***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tamprul

Artwork
Affra Gibbs

"The back door program included a feature that was designed to modify a computer in which the program was inserted so that the computer would be destroyed if someone accessed it using a certain password." - United States Department of Justice, July 1992

Writers: Bilisf, Eric Corley, Count Zero, The Devil's Advocate, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the irregulars.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Brock, Franklin, Bill, Al, and the DC crew.

Hackers in a World of Malls

SECRET SERVICE BEHIND HARASSMENT OF 2600 MEETING

It just hasn't been a good year for malls.

First there was the incident in June at a hacker gathering in St. Louis called Summercon. Mall cops at the Northwest Plaza told the hackers they weren't allowed to wear baseball caps backwards. The hackers, in their innocent naivete, questioned authority.

It happened again, this time at the Pentagon City Mall during the November 6th Washington DC 2600 meeting. But clothing wasn't the issue in this incident. Instead, the mall police didn't like the hackers' very existence. Or so it seemed.

It started like most other 2600 meetings - people gather at tables in a food court and start talking to each other. Remarkably similar to what real people do. But these were no ordinary people. These were hackers and the mall cops had plans for them.

Eyewitness Account

"At about 5:15 someone noticed two people on the second story taking pictures of the group with a camera. Most of the members saw the two people walk away with a camera in hand and we started looking around for more people. [One hacker] noted that he didn't like the guys standing up on the 'fed perch' on the second level and that they looked like feds.... At about 5:30... a mall security guard stopped me and told me to sit down because I was to be detained for questioning or some shit like that. I complied and waited. Now about eight guards were there surrounding the meeting. One guard approached the group and said that he saw someone with a 'scan gun' of some sort and would like to search the person's bag.... The scan gun turned out to be a Whisper 2000 listening device. Also the guard took possession of [a hacker's] handcuffs and asked what he needed them for and so on. At this point the guard asked for ID's from everyone. Most all people refused to comply with this order. At this time the guard called in to their dispatcher and their boss got on the radio and said that he was coming down to see what the 'hell is going on' with us. About two minutes later a gentleman in a suit arrived. Apparently he was the boss and he ordered the guards to get ID's.

"The guards used very coercive tactics to obtain ID's from threatening to call people's parents to calling the Arlington County police and having them force us to produce ID. They got ID's from most people, but some still refused to produce ID's. At this time a guard approached another person at the meeting and asked to search his bag too. This person gave consent to search the bag and the guard discovered a [legal] credit card verification machine. At this point the guards noticed to to call the Arlington County Police. About 10 minutes later the police arrived, demanded, and got ID's from the remaining holdouts and the mall security quickly wrote down all pertinent information from telephone numbers to social security numbers to date of births and addresses.

"The guards at no time disclosed what would be done with the information and responded that it was 'none of your business' when I inquired about it. When I asked about the illegal searches they were conducting they stated that they were within their rights because it was private property and they could do 'whatever we want, and you'll play by our rules or we'll arrest you.' Arrest me for what I haven't a clue. I asked why they seized the papers and electronic equipment from the bags and they said that it was 'evidence' and could be retrieved when they want us to get it. A wireless telephone bug was seized from my person.... I told them that it was a wireless intercom modification for a phone. When they said that they would keep it until Monday I pressed the issue that they were not entitled to it and I would take it now whether they liked it or not. At this time the guy in the suit said, 'Bring it here and let me look at it.' In his infinite electronics wisdom [he] concluded that it would be OK for me to have it.

..."During the entire episode a rather large crowd had gathered in the mall, including several people who other hackers identified as Secret Service agents. I cannot confirm this however. Most of the hackers who arrived late were not allowed into the arena but many observed the officers with cameras and some had their film taken and were handled in a very belligerent manner by the mall cops."

What It Was All About

The actions of the mall police were outrageous in the eyes of most. Consternation was swift and plentiful. But if this were simply another entry in a list of stupid things that mall cops have done, it wouldn't really have much significance. And, as many of us already know, this was indeed a most significant event.

Bright and early on Monday, November 9th, Brock Meeks, a reporter for *Communications Daily*, called the mall police and spoke with Al Johnson, director of Security for the Pentagon City Mall. They had the following conversation:

Meeks: I'd like to ask you a few questions about an incident where some of your security guards broke up a meeting of some hackers on Friday (Nov. 6).

Johnson: They broke up some meeting of hackers?

Meeks: Yes.

Johnson: I don't know about breaking any meeting up. Who... first of all I can't talk to you on the phone, if you want to come in, I don't talk to the press on the phone.

Meeks: OK.

Johnson: Ahh... maybe you oughta call the Secret Service, they're handling this whole thing. We, we were just here.

Meeks: The Secret Service was part of this?

Johnson: Well, FBI, Secret Service, everybody was here, so you might want to call their office and talk to them. There's not much I can really tell you here.

Meeks: OK.

Johnson: Our involvement was minimum, you know, minimal.

Meeks: I see, but your folks were acting on....

Johnson: We didn't break anything... I... we didn't... as far as I know, well I can't say much on the phone. But I, well, somebody's awfully paranoid apparently. Where'd you get this information from?

Meeks: Umm.... from computer bulletin boards.

Johnson: Bulletin boards?

Meeks: Yep.

Johnson: When did you get it?

Meeks: I got it, ah, Sunday night.

Johnson: Sunday night?

Meeks: Yep.

Johnson: [small laugh] Ah, yeah, you gotta call the FBI and the Secret Service. There's not much I can do for you here.

Meeks: Ok, Al, if I come down there will you talk to me down there?

Johnson: No, I can't talk to you at all. Fact is, there's nothing to talk about. Our involvement in anything was minimal, I don't know where this information came from as far as bulletin boards, and breaking meetings up and you know....

Meeks: Well, the Arlington police were down there too, I mean I've talked to several of the kids that were involved.

Johnson: Um-hmmm.

Meeks: They said, that ah, members of your, of the mall security forces, ah, or security staff, searched them, confiscated some material and didn't give it back. Did any of this happen?

Johnson: Like I said, I'm not, I'm not able to talk to you... we have a policy that we don't talk to the press about anything like that. You can call the Secret Service, call the FBI, they're the ones that remodeled this whole thing, and you talk to them, we're out of this basically, you know, as far as I'm concerned here.

Meeks: Ok, is there a contact person over there that you can....

Johnson: Ah... you know, I don't have a contact person. These people were working on their own, undercover, we never got any names, but they definitely, we saw identification, they were here.

Meeks: They were there. So it was all the Secret Service and none of your own?

Johnson: Ah, nah, that's not what I said. But they're the ones you want to talk to.

Fallout

At the meeting, several attendees had overheard mention of Secret Service involvement by both the mall police and the Arlington police. There, though, was clearcut indisputable evidence. And it was even captured on tape!

> "There just wasn't enough time for a cover-up and this is what did them in."

Calls by other reporters yielded a different response by Johnson, who started saying that there was no Secret Service involvement and

(continued on page 24)

Cipher Fun

by Peter Rabbit

One of the most vulnerable sources of private information is a personal telephone listing. If this listing is lost, stolen, or copied by stealth, much mischief may result. The following presents a procedure for telephone number encipherment that is designed to frustrate most snoops. This procedure is an adaptation of a polyalphabetic substitution cipher devised by Giovanni Battista della Porta, a sixteenth century Italian cryptographer. Porta's cipher table used alphabetic characters; here, it has been adapted for numbers as a polynumeric substitution cipher.

Description

The polynumeric adaptation in its simplest form is shown in Table 1:

Table 1:

	NUMBER	
	0 1 2 3 4	
	==========	
	0-1	5 6 7 8 9
K	2-3	6 7 8 9 5
E	4-5	7 8 9 5 6
Y	6-7	8 9 5 6 7
	8-9	9 5 6 7 8

Table 1 shows six number rows, five of which are controlled by either of two key numbers located at the left of the table. The upper row, containing digits 0 to 4, found above the double line, always remains the same; the remaining five rows, located below the double line and containing digits 5 to 9, are each arranged in a different way. As arranged here, they are shown in their simplest form for purposes of explanation, but these arrangements are not recommended for use, due to their inherent periodicity; preferable arrangements will be shown in the following section. Regardless of arrangement, however, the encipherment will be reciprocal for all six rows. For example, in Table 1, in the first row, which is controlled by the key 0-1, the substitute for 7 is 2 (found above the double line); and the substitute for 2 is 7 (found below the double line).

Each of the five rows located below the double line may be arranged in 120 different ways, producing a large number (120^5) of potential encipherment tables.

Method of Employment

Table 2 shows five enciphering rows in disarranged order. The method of disarrangement illustrated uses an easily remembered phrase, in this case a nursery rhyme: "Mary had a little lamb it's fleece..." The order of the numbers 5 to 9 in each row is derived from the alphabetic order of the nursery rhyme letters as they appear in each row:

M	A	R	Y	H
7	5	8	9	6
A	D	A	L	I
5	7	6	9	8
T	T	L	E	L
8	9	6	5	7
A	M	B	I	T
5	8	6	7	9
S	F	L	E	E
9	7	8	5	6

Table 2:

	NUMBER	
	0 1 2 3 4	
	==========	
	0-1	7 5 8 3 6
K	2-3	5 7 6 9 8
E	4-5	8 9 6 5 7
Y	6-7	5 8 6 7 9
	8-9	9 7 8 5 6

The enciphering of a telephone number in this procedure will require the selection of an autokey number from 0 to 9. This single autokey number is chosen by, and known only to, the encipherer. In order to end up with an encipherment that resembles a genuine telephone number it is necessary to select an autokey number that will produce an encipherment not starting with 0 or 1. Using the example of 751-2600, examination of Table 2 shows that there are four autokey choices in this particular case: 4, 5, 6, or 7.

Let us encipher the telephone number 751-2600 by using the arbitrary autokey 6 plus the first six digits of the telephone number. Using Table 2,

KEY	6 7 5 1 2 6 0
TELNO	7 5 1 2 6 0 0
CIPHER	3 0 9 8 2 5 7

In the first line, 6 is the autokey and 751260 are the first six digits of the phone number. The enciphered number is 309-8257. Let us now decipher it in order to recover the original number - a simple procedure. We begin by placing the autokey 6 over the first number of the cipher:

KEY	6
CIPHER	3 0 9 8 2 5 7
TELNO	7

Using Table 2, we find 7, the first digit of the telephone number. This number is moved up and becomes the next key number:

KEY	6 7
CIPHER	3 0 9 8 2 5 7
TELNO	7 5

Each digit of the telephone number is moved up and becomes the key for the next number to be deciphered, until the decipherment is completed:

KEY	6 7 5 1 2 6 0
CIPHER	3 0 9 8 2 5 7
TELNO	7 5 1 2 6 0 0

Further security of the enciphered telephone number may be obtained by adding a seven digit number using non-carry addition or subtraction; that is to say, 8 + 2 = 0, not 10; and 0 - 8 = 2. (The units digit is used, but the tens digit is ignored.) For purposes of illustration let us use as the additive a seven digit number representing the date of the Great San Francisco Earthquake and Fire: April 18, 1906:

CIPHER	3 0 9 8 2 5 7
ADDITIVE	4 1 8 1 9 0 6
SUPERCIPHER	7 1 7 9 1 5 3

Subtracting the additive from the supercipher produces the cipher, which is then deciphered with the autokey and Table 2:

SUPERCIPHER	7 1 7 9 1 5 3
ADDITIVE	4 1 8 1 9 0 6
CIPHER	3 0 9 8 2 5 7

For obvious reasons, one should not encipher every telephone number in one's collection - only the most critical ones. As for area codes, they are best left unenciphered.

beginner's guide to minitel

by NeurAlien

From CORE-DUMP, a French hacker publication

The Minitel is only the terminal of the TELETEL network. We often say Minitel when we should say Teletel. The Minitel was at the beginning only a Videotex terminal. It could display only 40 columns and could do only videotex (there was no RETURN key for example). That was the shitty **MINITEL 1** (the first MINITEL 1 had an ABCD keyboard instead of an AZERTY keyboard as on every French computer, to show you how shitty it was).

Now there are a lot of Minitels.

MINITEL 1B: It can be set to 4 modes: Videotex, American TTY, French TTY, French TTY with Minitel's key.

MINITEL 2: It's nearly the same as M1B but it can display more precise graphics (DRCS graphics), can dial by itself, can communicate at 9600 bps with the computer (instead of 4800 for the M1B), can detect the ring and can be protected by password (which can be bypassed... *hehe!!!*)

MINITEL 5: Tiny Minitel for travel with LCD display and other features.

MINITEL 10: Old.... The phone is integrated into the Minitel.

MINITEL 12: The phone is integrated into the Minitel and you can make a Minitel responder (like a little videotex server). You can also protect this one with a password.

The display is made in 40 columns for the videotex mode. It can display characters or low-resolution graphics for the non-DRCS Minitels.

The Minitel protocol is called V23, data is sent to Teletel at 75 bps (that sucks!) and Minitel receives data at 1200. The settings are: 1200,e,7,1 (1200 bps, even parity, 7 data bits, and 1 stop bit).

The MINITEL Keys

SOMMAIRE (INDEX): Go to upper menu

REPETTITION (REPEAT): Display once again the screen.

SUITE (NEXT): Display the next screen/message

RETOUR (BACK): Display the previous screen/message

GUIDE (HELP): Display a HELP screen.

CORRECTION (CORRECT): Erase the previous character typed.

ANNULATION (ERASE): Erase the whole line of text typed.

CONNEXION/FIN (CONNECT): Tell the modem to be ready to answer to the carrier.

FNCT (FUNCTION): Key used to change the Minitel into another mode from the current. (Avoid the device plug connected to the computer or the device which restricts the access to T1 for example — hehe...)

ENVOI (SEND): Equivalent to RETURN but in videotex mode.

All of the functions described are up to the server which can interpret in the way it needs/wants the escape codes sent Videotex Codes

These are a set of escape codes which can be interpreted by the Minitel or the Minitel emulation program.

There are a lot of different kinds of characters: position codes, movement codes, repetition codes, character size codes, attribute codes, color codes, etc.

The Teletel Networks

Teletel is in fact only an add-on to some PAD to make TRANSPAC (the french x25 network) compatible with the V23 protocol. The PADs for the Minitel are called PAVI. These PAVI offer different services: the 3613 — also called Teletel 1 (T1), the 3614: Teletel 2 (T2), and the 3615 (T3). The prices increase with the Teletel number.

36 05 xx xx is a number for free but restricted videotex server (Teletel 0). When you dial a T0 number, you usually log onto a closed server which provides access only for authorized users. The 3613 is the number to dial on the phone to access from everywhere in France to the T1.

You dial it, then, when you hear the carrier, you hit CONNEXION/FIN. It legs you onto the TELETEL 1. Then a screen appears and invites you to type either an NAB or a local Transpac number in this format:

1 **<department [2] > <transpac node [3] > <address on the node of the server [3] > <sa>** where <sa> is a sub-address used by the server which can be up to 5 digit, it's usually not used. A NAB is a short name to which is given a Transpac number in the PAVI's routing tables. then you hit ENVOI and it connects you to the videotex server.

Inside Teletel

In fact, when you log onto a PAVI, you log onto a videotex PAD which can understand the Minitel's keys and can display videotex screens. That's all. On those PAVIs, you can use X3 commands (or X28). When you type the NAB, it connects you to the TRANSPAC address it has found in its routing tables which is set EQUAL TO <NAB>. The PAVI then is like any PAD.

How the server can detect if the user is connected via T1,T2 or T3 (or others)

When the PAVI make an x25 call, the x25 address of the PAVI

is given to the server. This address has this format: **6 <department> <node> <adr> 8 <digit from 1 to 9>** The last digit tells the server from which Teletel (3614, 3615, 3613, etc.) the user calls and thus, the server can provide a full, restricted, or closed access. (When a user calls from 3615, it gives money to the server. From 3614, nothing to the server. From 3613, it costs some money to the server.)

The NTI Facility

This allows a Minitel User to make international calls. With an NUI and an NUA, you can do this: call 3613, type as the service name your NUA preceded by 0 (example: 03132000000), hit SUITE (NEXT), type your NUI, hit ENVOI (SEND). Then it connects you to the NUA which has been given. The call is made via the NTI which checks the validity of the NUI and make the gateway between TRANSPAC on the other X25 network.

The NUI consists of six alphanumeric characters.

Conclusion

So, as you can see, this is a short introduction and if we decided to explain everything in the Minitel or in the Teletel network, we couldn't do it in one month even if we were working 25 hours a day. But we have some document about the escape codes, the network architecture, and so on which we will share if there's an interest. So, if you need something about that, contact me on 3614 code LEGEND (LEGEND is for example a NAB) and my BAL (mailbox) is NeurAlien. We are going to make a videotex and international x25 server and then it will be easier to contact us.

vehicle identification numbers

Beginning with the 1981 model year, the National Highway Traffic Safety Administration, Department of Transportation, required manufacturers selling over-the-road vehicles to the United States to produce the vehicles with a 17 character vehicle identification number (VIN).

This standard establishes a fixed VIN format including a check digit and applies to all passenger cars, multipurpose passenger vehicles, trucks, buses, trailers, incomplete vehicles and motorcycles with a gross vehicle weight of 10,000 pounds or less. The first three characters of the VIN are designated the WMI (World Manufacturers Identification). The WMI uniquely identifies the Nation of Origin, Manufacturer, Make and Type of Vehicle. The second section has five characters and has been designated the VDS (Vehicle Description Section). The VDS uniquely identifies the attributes of the vehicle such as Model, Body Style, Engine, etc.

The third section of the VIN is located after the check digit. It is eight characters in length and is called the VIS (Vehicle Identification Section). The first character represents the vehicle model year; the second character represents the plant of manufacture; and the last six characters represent the sequential production number.

Let's use 1FABP28A5FF143890 as a sample VIN. 1FA is the World Manufacturer Identification - 1 is the Nation of Origin, F is the manufacturer, A is the make and model. BP28A is the Vehicle Description Section. 6 is the check digit. FF143890 is the Vehicle Identification Section.

The check digit will always be the ninth character in the VIN. Assign to each numeric in the VIN its actual mathematical value and assign to each alphabetic the value specified below:

A=1, B=2, C=3, D=4, E=5, F=6, G=7, H=8, J=1, K=2, L=3, M=4, N=5, P=7, R=9, S=2, T=3, U=4, V=5, W=6, X=7, Y=8, Z=9.

Multiply the assigned value for each character in the VIN by the weight factor specified for it below:

1st=8, 2nd =7, 3rd=6, 4th=5, 5th=4, 6th=3, 7th=2, 8th=10, 9th=0 (check digit), 10th=9, 11th=8, 12th=7, 13th=6, 14th=5, 15th=4, 16th=3, 17th=2.

Add the resulting products and divide the total by 11. The remainder is the check digit. If the remainder is 10, the check digit is X.

Example

VIN Characters:
1 G 4 A H 5 9 H 4 5 G 1 1 8 3 4 1
Assigned Values:
1 7 4 1 8 5 9 8 4 5 7 1 1 8 3 4 1
Multiply by:
9 7 6 5 4 3 2 10 0 9 8 7 6 5 4 3 2
Add products:
9+49+24+5+32+15+16+80+0+45+56+7+6+40+12+12+2=411
Divide by 11:
411/11 = 37 4/11
Check digit:
4 (compare to character in 9th position)

The check digit (9th position) will always be a numeric or an X. The tenth position indicates the model year as follows:

B=81, C=82, D=83, E=84, F=85, G=86, H=87, J=88, K=89, L=90, M=91, N=92

2600 NOW HAS A VOICE BBS THAT OPERATES EVERY NIGHT BEGINNING AT 11:00 PM EASTERN TIME. FOR THOSE OF YOU THAT CAN'T MAKE IT TO THE MEETINGS, THIS IS A GREAT WAY TO STAY IN TOUCH. CALL 0700-751-2600 USING AT&T (IF YOU DON'T HAVE AT&T AS YOUR LONG DISTANCE COMPANY, PRECEDE THE ABOVE NUMBER WITH 10288). THE CALL COSTS 15 CENTS A MINUTE AND IT ALL GOES TO AT&T. YOU CAN ALSO LEAVE MESSAGES FOR 2600 WRITERS AND STAFF PEOPLE AROUND THE CLOCK.

U.S. SECRET SERVICE FIELD OFFICES

who watches the watchers

by the GCMS MechWarriors

Albany, GA	912-430-8442 RA	Miami	305-591-3565
Albany, NY	518 472 2824 RA	Midland, TX	915 683-6822 D
Albuquerque	505-766-3336	Milwaukee	414 291-3587
Anchorage	907-271-5148 RA	Minneapolis	612-348-1300
Atlanta	404-331-6111	Mobile	205-690-3851
Atlantic City	609-347-0772 RA	Montgomery	205 832-7601 RA
Augusta, GA	404-722-7294 D	Nashville	615-251-5541
Austin	512-482-5103	Newark	201 645-2334
Bakersfield, CA	805-861-4112 D	New Haven	203-865-2449
Baltimore	301 962-2200	New Orleans	504-589-4041
Baton Rouge	504-389-0761 RA	New York	212-466-4400x2184
Beaumont, TX	409-866-0776 D	Norfolk	804-441-3200
Birmingham	205 731-1144	Northern, VA	703-378 1975 D
Bismarck	701-255-2284 RA	Oklahoma City	405-231-4476
Boise	208 334 1403 RA	Omaha	402-221-4673
Boston	617-565-5640	Orlando	305-648-6333 RA
Buffalo	716-846 4401	Oxford, MS	601-236-1563 D
Canton	216-489-4400 RA	Panama City, FL	904 265-9323 D
Charleston, SC	803-724 4851 RA	Paris	4296-1703x3206
Charleston, WV	304 347 5188	Philadelphia	215 597 0500
Charlotte	704-523-9583	Phoenix	602-261-3566
Chattanooga	615-265 4014 RA	Pittsburgh	412-644-3384
Cheyenne	307-772-2380 RA	Portland, ME	207-780-3493 RA
Chicago	312-353-5431	Portland, OR	503 221 2162
Cincinnati	513-684-3585	Providence	401-331-6456
Cleveland	216 522 4365	Raleigh	919-790-2834 RA
Colorado Springs	303-594-4500 D	Reno	702-784-5354 RA
Columbia	803 765 5445	Richmond	804 771 2274
Columbus	614-469-7370	Riverside	714-351-6781 RA
Concord	603-225-1632 RA	Roanoke	703 982-6208 RA
Corpus Christi	512-888-3401 RA	Rochester	716-263-6330 RA
Dallas	214-767-0027	Rome	4674 x2694
Dayton	513-252-3013 RA	Sacramento	916-551-2802
Denver	303-844-3027	Saginaw	313 234 7223 RA
Des Moines	515-284 4565 RA	St. Louis	314-425-6230
Detroit	313-226-6100	Salt Lake City	801-524-5810
El Paso	915-543-7640	San Antonio	512-229-6175
Flint, MI	313-234 7223 D	San Diego	619-557-6640
Ft. Myers, FL	813-337-3566 D	San Francisco	415 556 6300
Fort Smith, AR	501 452 4482 D	San Jose	408-291-7220 RA
Fort Worth	817-334-3015 RA	San Juan	809 753 4539
Frederick, MD	301 293 1958 D	Santa Barbara	805-963-8930 RA
Fresno	209-497-5204 RA	Savannah	912 944 4431 RA
Grand Rapids	616 456 2276	Scranton	717-346-5781 RA
Great Falls	406-453-9515	Seattle	206 442 5405
Greenville	803 233 1490 RA	Shreveport	318-226-5299 RA
Harlingen, TX	512-428-0311 D	Sioux Falls	605-331-4565 RA
Harrisburg	717-782-4611 RA	Spokane	509-456-2532
Honolulu	808-541-1912	Springfield, IL	217 492 4033
Houston	713 229 2755	Springfield, MO	417-864-8340 RA
Indianapolis	317-269-6444	Syracuse	315 423 5338
Jackson	601-965-4496	Tallahassee, FL	904-877-0865 D
Jacksonville	904-724 4530	Tampa	813 228-2636
Kansas City	816-426-5522	Toledo	419-269-6434
Knoxville	615 673 4527 RA	Towson	602-629-6823 RA
Las Vegas	702-388-6446 RA	Tulsa	918-581-7272 RA
Lexington	606-233-2458 RA	Tyler	214-534-2908 RA
Little Rock	501-378-5241	Waco, TX	817-848-4545 D
London	499-9000x3264 RA	Washington	202-634-5100
Los Angeles	213 894 4830	West Palm Beach	407-659-0184 RA
Louisville	502-582-5171	White Plains	914 682-6161 RA
Lubbock	806-743-7347 RA	Wichita	316-267-1462 RA
Madison	608-264-5191 RA	Wilmington, DE	302-573-6188 RA
Melville	516-249-0404 RA	Wilmington, NC	919-343-4411 RA
Memphis	901-521-3583	Youngstown, OH	216-746-0180 D

RA = Resident Agent, D = Domicile

Letter From Prison

The following information comes to us from a prisoner in California. We've removed the name and location to protect their identity.

I would like to let you know how much I enjoy your magazine. My opportunities to enjoy computer "fun" and phreaking are about zero right now since I am engaged in involuntary solitude. It is with some interest, therefore, that I have followed your reports of rejection by federal prisons and by the Texas Department of (sic)Corrections. As you now know, prison inmates whose First Amendment rights are protected only by federal law have a tough way to go. The Federal Prison Rulebook allows a warden to reject a publication "if it is determined detrimental to the security, good order, or discipline of the institution or if it might facilitate criminal activity." This rule was held valid under (in spite of?) the Constitution's First Amendment by the U.S. Supreme Court (Thornburgh v. Abbott (1989) 490 US 401, 104 L Ed 2d 459, 109 S Ct 1874).

Much to my delight (and surprise) it seems that the great state of California is somewhat more liberal about prisoners' rights to read "questionable" literature than the federal standard. California Penal Code, sections 2600 (j) and 2601 are, together, sometimes called "the [California] prisoner's bill of rights". The only restriction on reading material is a restriction against printed matter which depicts the manufacture of weapons, explosives, poisons, or destructive devices, or which depicts sexual assaults against Department of Corrections employees. No other subject matter can be legally excluded.

Lest you think that the First Amendment is completely healthy in California, here are some examples to show that it is not: A friend of mine was recently refused two issues of *Hustler* magazine. One issue had an article on Asian street gangs in the U.S.A. The other had an article about female inmates in the California Youth Authority (convicted delinquent children) being raped by staff members. Both articles were called "a threat to institution security". Sound familiar? Mailroom personnel here have clearly exceeded their authority and the case is headed for court.

Two years ago I was refused a Loompanics book catalog because pages 65-66 were not allowed. I later discovered that the offending pages contained a tongue-in-cheek article on how to use the catalog itself as a weapon!

A friend of mine was denied a book on computer hacking which he ordered from Loompanics. He did not contest the refusal, but should have. I received *Out of the Inner Circle* by Bill Landreth with no problem.

The exclusion of "unsolicited advertising" literature allowed by CCR, sec. 3143(a)(1) is also much abused. I sent in reader service cards to *Byte* and *Popular Communications* magazines requesting 42 different brochures. I received one reply. One year later I sent off again, this time for 84 brochures. I also informed the mailroom in advance that the brochures were coming. It's been six months now with no responses so I guess it's time to sharpen up my pencils and oil up the typewriter. (Electronic typewriters are not allowed here. They are terrified that we will hide something in the 4K RAM and they won't know how to access it.) Still, we at least have a fighting chance to beat the censors. A considerable body of case law exists to support P.C. 2600 and 2601. If I can't play with phones and computers I might as well learn about the law.

Prison Phreaking

I have not tried phreaking here and probably will not (will not be able to, I mean). All phones have "this phone is subject to being monitored" signs above them. A beep tone sounds at 15 second intervals. Occasionally the monitor circuit can be heard clicking on. Phones can be turned off and on remotely from a single, central, location. The phones themselves are of a type very common as payphones. They are approximately 21 inches high by eight inches wide by seven inches deep; black case with blue front plate; no coin deposit slot but does have a coin return slot; a Bell System emblem is on the right side of the blue front plate about halfway up; coin return piece says "Bell System - Made by Western Electric" on it. The local carrier is Pac Bell and the long distance carrier is MCI as of about two years ago. Prior to that it was AT&T. Calls are collect only. Alternate carrier access is blocked as is 500 access. 10777### brings a

"Electronic typewriters are not allowed here. They are terrified that we will hide something in the 4K RAM and they won't know how to access it."

ringing signal and a recorded message saying, "An alternate carrier access number is not needed to complete this call. Please hang up and place your call again." 10333### brings the same. Dialing an 800 number brings a recorded message that says, "This call cannot be completed as dialed."

A normally placed call from here (collect) is placed in the standard way: 0, area code, plus seven digit number and brings on a live operator identifying him/herself as an MCI operator and asking for the caller's name. They then disappear and check for call acceptance without the caller hearing any conversation with the called party until after the call is accepted. I was quite interested in the letter on page 29 of Volume 7, #3. Perhaps I can look forward to automation in the future.

Normal access to local directory assistance (555-1212) is also blocked. A recording informs the caller that the number cannot be reached. I tried 555-1212, 411, plus 555-1212 with my area code, and preceded by 1 and 0. These all bring up prerecorded rejections except for the last (0+) which brings on an MCI operator who sounds perplexed that anyone would try to call collect to directory assistance and says they won't accept collect calls.

Long distance information, anywhere in the U.S.A., is available by dialing (area code) 555-1212, with or without a 1 in front. Best of all it's free. Sometimes local information can also be obtained by dialing information in an adjacent area code. As I said, alternate carrier access is blocked here, but another prison I was in had 10777### and 10333### direct access to alternate carriers. Unfortunately this access was blocked due to "overuse". We switched to an 800 access number until, finally, all 800 access was blocked. The fun lasted about one year. At the time my wife had a legitimate Sprint card (which supplied the 800 access number) and I usually used her legal code number to call home (I was more cautious than most). We discovered that 10777### leaves a calling phone number record which appears on the bill. Using 800 access causes the bill to say "western wide area access call" in the calling number column of the bill. These cost 75 cents extra over direct access calls.

We also tried having people direct dial to the jail payphone to avoid operator assistance charges yet still be legal. But the phones were blocked to incoming calls. They did not even have their numbers posted on the phones. We got it off of phone bills. To this day I marvel at the nimble-fingered few who could come up with valid 9 digit Sprint codes in 10 to 15 minutes. There is magic there. I could do it in an average of one and a half hours. I would blunder around with a "used up" nine digit code number until I got a valid first seven digits (I made it through code number and 10 digit phone number before getting reject tone) then plodded along through the 100 possible combinations of last two digits (00 to 99) until a "hit" occurred. It was slow, grueling work but god damn it somebody had to do it after "Nimble Fingers" went home.

Interestingly enough, Sprint seemed to prefer an electronic war rather than working with law enforcement. On occasion jail guards were spotted watching phones (from 50 feet away) with binoculars as guys dialed. On another occasion two guards rushed a guy who had been dialing continuously for over an hour and took his notes away from him (a 00 to 99 grid) but nothing came of it. A lieutenant in the jail even said that they had called Sprint repeatedly with information, in case Sprint wanted to prosecute, but "they didn't seem to care". However, we lost 10777### and 10333### access. Once, at about number 17 while running a 00 to 99 sequence, I had an operator come on the line asking if I was having a problem. I switched to random number choice on the grid and had no more problems. But the code numbers were going dead in shorter and shorter time spans. Before loss of 800 access killed our fun the code numbers were lasting only two or three days. There is a proposed bill which could grant the Director of Corrections the power to choose which long distance carrier to use in all California prisons. Think of the revenues involved! There is a 15 to 25 million dollar per year payback to the prisons for supplying phone locations (to captive customers with no choice of alternate carrier and no other way to call than "collect"). This money may be up for grabs soon and screw the poor families who are forced to pay the "operator assistance" charge for all calls or else forgo phone calls.

A logical compromise to the high expense vs. phone fraud problem would be to allow use of "Call Me" cards, which can only be used to call the card holder's home number yet avoid operator assistance charges. But it is difficult to establish meaningful communication with minds that ban TV remote controls because "transmitting devices" are forbidden in California prisons, and electronic typewriters are considered a "threat to institution security".

We used to have a large collection of California phone books in our library. They were all locked away when a guard supposedly found his own home address listed in one. This place makes me think of the sign I once saw: "Help, the paranoids are after me."

GROWTH OF A LOW TECH HACKER

By the Roving Eye

About a year ago I wrote an article about the birth of a hacker in a low technology atmosphere. A lot has happened since then. For one thing I have been able to meet with hackers from the area. For the other I have been able to gain some hacking experience. These two combined have led me to appreciate a "problem that exists in our community" (pardon the sap). Hence this article.

I find that a lot of newcomers to the field have no idea where to turn, hacking being no product of corporate America which is blared across our TV screens every five minutes. Thus, if you are a newcomer, read this! You probably will not find much else! Hacking is first and foremost a time-consuming enterprise. It requires tireless devotion as well as relentless perseverance. This is why you will never beat that curious kid next door who started letting his curiosity take him places when he was too young to pay for 2600 out of his allowance. This is also why a newcomer finds it hard to get around in this neighborhood. If you are not serious about hacking and intend to let your "determination" quiver after six months, leave now. Hacking is not a hobby, it is something that stays with you for life. If you are serious, then there are very few gaps that you will not be able to fill in with hard work. But like everything else in life, it is also important to work smart. Here are some pointers that I have come up with from my own experience:

1. Definitions first. It will help you a lot if you define to yourself who you are, what you are interested in doing, what your goals and priorities are, what sacrifices you want to make, and what lines you are not willing to cross. In this respect, hacking is a discipline. You will waste a lot of time or feel rotten if you skip this most important step. I personally decided that I support the free flow of information, but I do not believe in even risking harm to others. I do not believe in following the law, but I do believe in living honestly. I believe in what is right, not what is just.

2. Stop doling out information now. Living in this society, almost every minute we announce ourselves to the world. Stop letting out information to the world. Unless absolutely necessary, use a false name. And don't reveal your social security number to every Tom, Dick, and Harry. I usually use two Hindi swear words, and not even Ma Bell had a problem issuing me a calling card. Can there be a more silly point than this to make? Yet this advice went unheeded and a boastful friend of mine is in big trouble. Arrogance is never worth it.

3. Get others working for you. This country is full of people waiting to give you stuff for free. Use them, abuse them, and you will even get thanked for it! Call the FCC and get put on their mailing list. And this does not apply only to the electronic frontier. Tourist offices will love to cover your walls with their awesome

posters. The fed would love to tell you everything the *Wall Street Journal* can tell you, and more, for free. You just have to appear to be corporate and know how to ask.

4. Use the easiest way. AT&T does not want you to know a lot of things. But for most of these you need not break into their computer or even think of a great scheme. A little social engineering will do the trick. I called their 800 number and asked about ANI. They kept transferring me from office to office, until I got them to give me the number of the AT&T FIND service, an internal number that employees use to find out technical information. *And they even paid for the calls I made to them.* No blue boxing, nothing illegal.

5. Play on people's ignorance. If people weren't stupid, hacking would be nearly impossible. Try simple insecure passwords. Assume insecure networks and sites. I have even managed to get system access to a computer by logging in on telnet as anonymous! Talk fast to the AT&T operator and tech support, and they will tell you the DTMF codes! Do not assume that these people have any brains at all!

6. Use all the legitimate resources you can lay your hands on. Learning UNIX out of a book will not teach you much about hacking, but it will give you the tools to your art. Approaching hacking without some of this kind of formal support is like trying to learn C by reading the comp.lang.c Usenet newsgroup. Learning UNIX security from a text will not only accelerate your progress, it will also make your skills valuable in the outside world.

7. Get a feel, and then get a plan. Perhaps I should have put this higher up in the list. But I purposely left it for down here. The above pointers should help you get an idea of our world. But then you must step out and do something for yourself. Play with an arm tied behind your back. Increase the challenges. But whatever you do, get a plan. I wasted a lot of time because I was doing some serious dabbling in stuff I could not give two hoots about. A plan helps one go right back to the definitions stage... where it all begins.

8. Work cheap. My poverty has proved be my greatest asset. No one can afford Radio Shack, no matter how rich they may be. Not because RS is that expensive, but because the maxim of more money, more hot air holds very true here. The more money you plan to spend, the more bullshit you will be fed. If you buy cheap, you will learn more by doing things yourself. You will value your equipment. And you will have more of it.

9. Get friends... use the resources. Before I started reading *2600* and *Phrack*, I had no one to turn to with my problems, no one to guide or encourage me. Re-inventing the wheel may have its virtues, but riding a sports car that you built from a kit is a lot more fun!

10. Review. If you want to get anything out of this for the long run, review what you have done. A present problem may have been solved in the past. Take account of what you have learned. Know where you stand. And *bash on regardless.*

HIGH TECH HAPPENINGS

The Hacker "Threat"

We thought it would be amusing to share some leaked information that was received in Holland from Lawrence Livermore Laboratory and then passed over to us. It concerns the potential threat that Dutch hackers pose to the free world.

"At least some of the Netherlands attacks originate from Eindhoven University. Our hacker sources also allege that there are actually two sets of attacks. In the first set of attacks the attackers may be using X.25 carriers to access a machine called "LC" or possibly "ELSIE" (we have since learned that there is a domain of computers at MIT with the address of lcs.mit.edu). From LC or LCS, there is a phone connection to TERMINALS at MIT.... The first set of attacks may, according to our hacker sources, yield accounts to more systematically penetrate later. The second set of attacks is through an unknown route. During these attacks someone apparently breaks into accounts discovered during the first set of attacks and transfers files. One hacker claimed that a hacker from the Netherlands was bragging that he had been using AUTOVON, the unclassified U.S. military telephone network, to break into systems; subsequently, other sources within the U.S. Army have informed us that they have recently found that AUTOVON has been illegally used for data transfer between computers. Our hacker sources claim that two Dutch individuals, Rop (alias "Ron") Gonggrijp and Maurice Katz, are principal players in these attacks, although there may be as many as twelve hackers involved. Gonggrijp is allegedly a contributor or co-editor of Hacktic, a magazine for hackers, in Amsterdam. He is linked with the second set of attacks. He is the individual who allegedly has bragged about his ability to break into the AUTOVON system. Army Intelligence describes him as hardened and capable of making considerable trouble. In one electronic conversation two months ago with a system manager at the University of Chicago, a person identifying himself as "Ron" claimed he has spent one year in jail (three days ago the FBI informed me that "Gonggrijp" is an alias). Gonggrijp is, according to our hacker sources, presently in the United States on business. Maurice Katz is an alias for Marcel P. K., a 23-year old who lives in the Netherlands. He allegedly is responsible for the first set of attacks. His resume indicates that he is interested in the United States defense system, and several sources have informed us that he will be travelling to the United States within a week to interview for computer-related jobs with defense contractors. According to these sources, K. was fired from his job as system manager at Eindhoven University. Some time later he allegedly destroyed a number of

systems at Eindhoven in retaliation. Our hacker sources have informed us that both individuals have had a substantial increase in standard of living over the last few months. Both are said, for example, to travel more frequently and to now travel first class. Several sources maintain that either One Magazine or Der Spiegel in West Germany is paying these individuals a large sum of money for military information for U.S. computers. This information allegedly will be published in one issue, although one unidentified source suggested that countries hostile to the U.S. are supplying the money and funneling it through one of these magazines."

This was actually written a couple of years ago and nearly everything they consider to be fact has been proven false. Since we know the people accused quite well, we can say confidently that this is all a load of garbage and probably entirely based on hearsay or wishful thinking. But this is dangerous garbage because it comes from powerful people and is sent to even more powerful people. And there is nothing more dangerous than a group of powerful paranoids.

Foulups and Blunders

The computer that selects people for federal grand juries somehow reached the conclusion that everybody in Hartford, Connecticut was dead. It actually happened because the "d" in Hartford somehow slipped into a column where a "d" meant "dead". Apparently, federal workers grew curious as to why nobody from Hartford ever seemed to be selected for a grand jury.

Hartford has been dead for the past three years.

Late last summer, the presses at De Gelderlander (a Dutch newspaper) stopped functioning, resulting in delayed deliveries. Lots of angry subscribers called the paper by dialing its phone number: 650611. The number got jammed, resulting in only the last four digits getting through in many cases. It just so happens that 0611 is the national emergency number in the Netherlands. You can probably guess the rest.

According to a computer that's supposed to log these things, a freeway emergency phone in Orange County, California had 25,875 minutes of calls attributed to it. We don't know how many of those minutes were emergencies but the calls spanned the globe.

Advances in Technology

In December, British Telecom launched a new redesigned telephone bill, designed to be simpler and more understandable. According to British Telecom, new elements of the bill include the following: information is presented in a clear, logical way; the front sheet summarizes the charges, which are detailed on subsequent sheets; clear language replaces obscure jargon and codes; the format contains details of customer options and itemization; the itemized pages spell out the locality of the called number; on the summary sheet, charges appear on the left so the eye alights on them first.

The New Jersey State Senate has voted 31 to 2 to expand the state's wiretap laws to allow tapping of beepers, modems, and fax machines.

SouthWestern Bell customers in Kansas and Missouri can now ask for zip codes whenever they call information in their area code. It seems logical that anyone calling information in these two states would be able to get zip code information since they'd be connecting to the same information operators. But, according to SouthWestern Bell, this is only a local thing.

According to the Network Reliability Council (an FCC advisory group), local and long distance phone companies have had 91 major outages since April, each of which affected at least 30,000 lines.

The Postal Service is getting a new voice network. It will consist of Northern Telecom Meridian 1 PBX's and AT&T and WIN Communications key systems.

Prophone - National Edition is a collection of three CD-ROM's from ProCD supposedly containing most of the nation's residential and business telephone directory listings. It consists of one business CD and two residential. It's available for only $349, a fraction of what Bell Operating Companies have been asking for such information. ProCD is reachable at (617) 631-9200.

AT&T has a new service called Fax Mailbox, which allows users to get faxes while traveling. Any AT&T calling card holder can get a mailbox number where faxes and voice messages can be stored. They can be retrieved through an 800 number for 70 cents a page or 35 cents per message.

The following appeared in our local newspapers: "On November 2, 1992, AT&T filed tariff revisions with the Federal Communications Commission to reduce the number of Special Rate Occasions (occasions when special lower rates apply to Evening and Night/Weekend Dial Station calls) from ten (10) Evenings and nine (9) Night/Weekends to zero (0), and to reduce the number of Floating Holidays (those holidays over and above the regular ten (10) federal holidays) from four (4) to zero (0)." If we're able to successfully read into this, it appears that AT&T is doing away with all holiday rates. If this is so, it's hard to imagine why more of a fuss hasn't been made. If it's not so, it's high time these announcements were printed in English so people can understand what they're trying to say.

Modem Mate I is a device made by Phonetics of Aston, PA to supposedly foil hackers. According to their brochure, "The device answers the

phone with a realistic-sounding 'Hello.' The hacker will not realize that a computer system exists on the other end and simply hang up [sic]. Only someone who knows what to do can gain access to the modem." Modem Mate II uses Caller ID to deny access to anyone not on the list.

Northern Telecom is allowing end users to restrict calls themselves using an authorization code rather than go through the phone company. So far, this is being tested on DMS-10 switches.

It's now possible to use Visa cards to pay for calls from British Telecom phones in the United Kingdom by dialing 144. The Visa card can also be used to call UK Direct from other countries. Before using the card, callers will have to get a four digit PIN which will differ from the PIN used to withdraw cash.

Abuse of Power

It's interesting how the government wants to treat copies of electronic documents as valuable property when they're prosecuting computer hackers. However, Bush and Reagan administration people want to destroy the White House's electronic mail, claiming it's not the same as files that would ordinarily be preserved in the National Archives. Many people rightfully believe that such electronic mail provides valuable insight into how this country is run, as demonstrated during the Iran/Contra hearings. For the moment, democracy is safe; a federal judge has ordered the Bush White House staff not to delete anything.

As of January 1, 1993 all driver license renewals require a Social Security Number in the state of California. The SSN is not printed on the license, nor is the digitized thumb print everyone is now required to get.

Numbers

Here are Cable & Wireless access numbers from overseas:

Australia: 0014-800-127-195
Bahrain: 800-113
Belgium: 078-11-8845
Denmark: 8001-8749
Finland: 9800-112-40
France: 05-906701
Germany: 01308-17976
Greece: 00-800-122-394
Hong Kong: 800-3072
Hungary: 00-800-11627
Ireland: 1-800-557-002
Indonesia: 00800-015-7338356
Israel: 177-150-1367
Italy: 1678-71361
Japan: 0066-33-810-072
Luxembourg: 0-800-4399
Malaysia: 800-0338
Netherlands: 06-022-6436
New Zealand: 0800-446636
Norway: 050-12890
Portugal: 0501-8-13-694
Singapore: 800-9886
South Korea: 008-14-800-00-57
Sweden: 020-792-558
Switzerland: 155-09-16
Taiwan: 0080-14904-8
Thailand: 001-800-13-733-8769
United Kingdom: 0800-89-2305

This ad was found at a truck stop. The rates may be slightly higher than other companies but not having a monthly fee may offset this.

SECRET SERVICE SCANDAL

(continued from page 6)

that he had never said these words. He was unaware at the time that a tape recording of his comments existed. When this fact became clear, Al Johnson faded away from the public spotlight. The obvious conclusion to draw is

that superior Meeks got to Johnson before the Secret Service was able to. In fact, a couple of weeks later at a hacker court appearance in New York, a Secret Service agent would be overheard boasting on how badly they had screwed up in DC.

Very few people failed to see the significance of this latest Secret Service action. Outrage was expressed in many different forums, over the Internet, on radio programs, over the phone, through the mail, and in independent media outlets. Mainstream media (as usual) missed the boat on this one. While the story did manage to make the front page of the *Washington Post* (November 15), the issue of Secret Service involvement in illegal searches and intimidation tactics wasn't gone into nearly enough. There was no mention of the person who had film ripped out of their camera for trying to document what was happening. Nor was there mention of the person who tried to write down the names of the cops and wound up having the list seized by them and torn up. Rather, this seemed to be accepted as standard practice and what was unusual, and even news for concern, was the fact that hackers actually mingle with the rest of America in shopping malls. It's probably not necessary for us to point out the dangers of accepting what the Secret Service did to us. Most of our readers know that accepting one atrocity as the best way of ensuring another. If we allow a small piece of our freedom to be taken away, the hunger pangs for another piece will be even stronger. That is why we will not tolerate such activities and that is why we have begun to fight back.

Our Plans

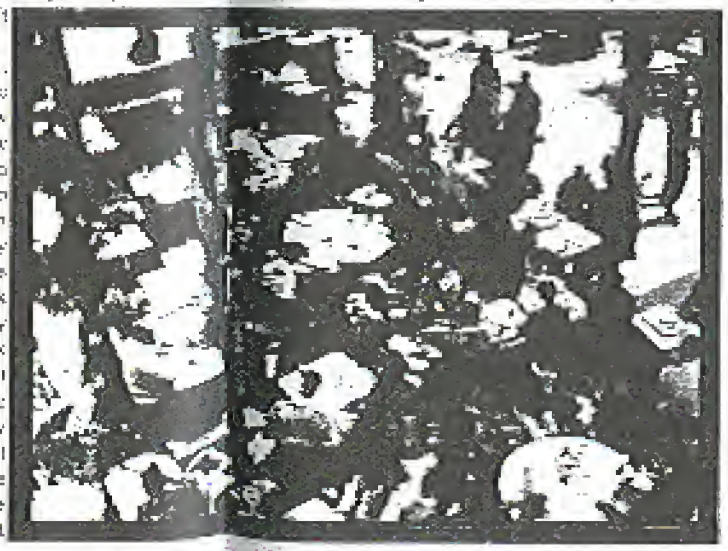
While a mall can technically be considered private property, in reality it is an area where the public gathers. In a large part of our country, malls have replaced town squares as places to meet and see your friends. We have trouble with, and don't intend to passively accept, policies which allow people to be removed from malls simply because of who they are. This is especially repugnant when the people are mall customers who aren't even being accused of anything!

We intend to continue meeting in such areas and will only stop when it becomes illegal for anybody to meet in such a place. Since we have meetings all over the country and have had them in New York for more than five years without incident, we don't really anticipate this to be a problem. In fact, we doubt we ever would have had a problem at the Pentagon City Mall if the Secret Service hadn't "manufactured" their way through.

At the December meeting, hackers from New York came to the Pentagon City Mall to show support. A total of about 75 people came to this meeting, ranging from 12 year old kids to people who read about it in the *Washington Post*. The mall cops stayed away and there were no incidents (except that they threw out Brock Meeks for asking too many questions and for trying to track down Al Johnson). We don't anticipate any problems at future meetings here. The Pentagon City Mall is a great place to get together and we intend to continue meeting there. We also estimate that our little group spent about $1000 in the food court alone.

We have a saying at *2600* that seems to hold true for each time we get hassled or challenged. Every time we're attacked, we only get stronger. This latest incident is no exception. We've had more people from various parts of the country contact us wanting to start meetings in their cities. Attendance at the existing meetings has gone up. And people "outside the loop" are finally beginning to see that hackers are not criminals. After all, do criminals meet openly and welcome outsiders?

In addition, there is now the question of legality. Every legal expert we've spoken with tells us that the Secret Service and Pentagon City Mall actions are clearly outside the boundaries of due process. Those responsible may only now be realizing the potential legal trouble they're in. It's very likely they thought that the hackers would be intimidated and wouldn't tell anybody what happened. Perhaps this train of thought works when the intimidated parties are criminals with something to hide. In this case, the hackers immediately got in touch with the New York *2600* meeting, the *Washington Post*, the Electronic Frontier Foundation, Computer Professionals for Social Responsibility, and the American Civil Liberties Union. Word of the harassment swept across the nation within minutes. The authorities were not prepared for this. There just wasn't enough time for a cover-up and this is



what did them in.

Freedom of Information Act requests (FOIAs) have already been filed with the Secret Service. This is the first of many legal steps that are now being contemplated. It's time we put a stop to this abuse of power and it's also time for the Secret Service to stop sneaking around shopping malls spying on teenagers and start getting back to something important.

For those of you interested in starting up meetings in your city, we ask that you contact us by phone at 516-751-2600. We don't have a whole lot of guidelines but we do ask that you use common sense. Pick an open setting with plenty of space and access to payphones. It's far preferable if the payphones can accept incoming calls. Unfortunately, you must be prepared for the kind of unpleasantness that took place in Washington DC. The mature and professional reaction of the DC hackers is what really made the difference in this case.

As far as what actually goes on at a *2600* meeting, there are no rules. Obviously, it's best if you don't cause any problems and don't do anything illegal. New people should be welcomed, regardless of their views or your suspicions. All kinds of information should be shared without fear. But most of all, meetings are for the purpose of getting hackers openly involved with the rest of the world so they can see for themselves what we're all about. Since it's obvious the media won't soon dispel the myths, it's really up to us now.

feedback

Federal Issues

Dear 2600:

To the Fed: I read your article in the Summer 1992 2600 on how you say you work for the federal government (Treasury Department to be exact) and how you got on hack/phreak boards because you told the truth and the sysops just let you on.

I can tell you this. I run an h/p board here in Maryland (home of the NSA) and can tell you that if I knew that you worked for the feds or even had any contact with them I never would have let you in. I know that there might be the chance that feds are on my board of 140 users but I sure don't know about it. If I did they'd be Gone like The Wind.

I have nothing against you and I'm sure that you're a pretty cool person. It's just that I'm upset that a person who out and out said that they were a fed, is even given the time of day by some dumb ass sysop. Maybe one day the 14 year old sysops might wise up to the facts.

Albatross

Credit Problems

Dear 2600:

First I would like to state that the information that I'll be asking for is for informational purposes only.

Which back issues, if any, would have the most information concerning credit reports and/or credit bureaus?

Also could you put me in contact with anyone or any group that may be expert in this field?

If you feel I need to be a little more specific, I'm talking in terms of being able to clean up one's credit report. Again, for informational purposes only!

D
Nederland, TX

Dear 2600:

I have just received my first issue of your magazine and I'm finding it incredible. It made me realize how much I still have to learn, but no harm in learning. But the real reason I'm writing this is because I have a problem with TRW credit. After a long lengthy court battle, in which they lost, they still have yet to restore my credit rating. Quite frankly I'm pissed off. Who do these people think they are? I've been trying to find some way of entering their computer and restoring my credit.

BR
Hamilton, ONT

Dear 2600:

Congrats on a cool 9:2 issue, 2600 has to be the most relevant zine in print. I've got a request for help. Nothing drastic, but my credit is getting hacked by a major corp. Used to work for Motorola, doing s/w for new chips.

When they started drug testing, I spoke out along with others and filed a lawsuit. Eventually, we won the suit and eventually I quit. But in the meantime, Moto also pulled stunts like losing paychecks, making drug accusations while I was under cross-examination, having an exec "remind" me that people can get "hit" for only $300 in this part of the country, etc.

Over a year later, just after participating in a second lawsuit against Moto, I got a notice from AMEX about "my new credit card". I hate AMEX and never do biz with them. Sure enough, a card had been issued in my name and the papers came from Motorola, applied for by one of their local managers five days after my second suit had been filed. I got the card stopped, no charges on it so this won't cost me money. I checked with AMEX and they claim it's all my fault because I'd been a Moto employee and had given them my SSN for tax forms. The manager claims it's just a database error and that all employees were supposed to get corporate cards, my employee records hadn't been purged, etc.

The above statements may be true, but they lead to interesting questions. First, I'm more than a little pissed that the police wouldn't even listen to the case. AMEX won't reveal my credit application forms, and so far no lawyer will even touch this issue without major bucks, which I can't afford. If you or I had hacked some corporate exec's credit this openly, we'd be in a jail now. Ergo, another example of corporate immunity from laws designed to curb individuals.

Second, how many years have to pass before use of my SSN by a former employer is no longer considered a "mistake"? Can all of my former employers file credit applications in my name without legal recourse, ad infinitum? Are there federal statutes which apply against the keeping of database records for "fraudulent purposes"?

Third, should I just drop this and catch up next time it happens?

I mean, I can file a lawsuit for a "cease and desist" order against Motorola's use of my SSN without a lawyer, but are there any other actions recommended?

I realize this may not be quite your domain to answer questions, but I thought you might be familiar with the issues.

Pacold

Americans are slowly waking up to the fact that the current credit system is horribly unfair and arbitrary. We believe if an agency is going to make money selling information about you, you should have the right to see it and correct any errors without having to go to a lot of trouble. Currently, the consumer has to do all of the work. And a lot of consumers would correct their credit reports themselves if they knew how. But, in today's world, accessing and correcting your own credit report (which was started without your permission) would be a violation of the credit agency's privacy.

Concerning the problems above, the solution is to be loud and vocal and send lots of certified letters. We cannot access people's credit files for them nor can we recommend people who can. If you just want to see what the formatting looks like, we suggest reading our 1984 issues when this whole thing first came to light. Things haven't changed all that much since then. In the last letter we would suggest filing a court order against Motorola to prevent them from using any of your personal information. We welcome other suggestions.

What a Surprise

Dear 2600:

I recently came into contact with your magazine for the first time (the Summer 1992) issue. Now, I first started programming in 1977 (which I suppose makes me a hopelessly outdated relic to some people) when the word "hacker" had a very different meaning, and there was no danger in uttering the words, "I am a hacker."

To my shame, my first thought when I saw 2600 was, "It's probably full of adolescent rants denigrating those who don't agree with the authors' particular points of view, and boasts about their "hacking" abilities, peppered with words like "kewl" or "awesum."

I was quite pleasantly surprised when I found my initial knee-jerk reaction to be almost completely unfounded. 2600 contains quite a bit of interesting reading, written by articulate, intelligent individuals.

I was so impressed that I intend to subscribe. Keep up the good work!

JL
Tampa

Lots of people have similar reactions upon meeting their first hacker.

More Simplex Shenanigans

Dear 2600:

It seems that several hospitals belonging to the same medical community have decided to install Simplex locks in several "High Security Risk" areas. These include places like the pharmacy, data processing department, and medical records just to name a few. The 2600 press release concerning the Simplex lock problem was given to those in charge, and they replied that because the doors in question were inside the building it wouldn't be a problem.

Cray-Z Phreaker

How nice that everybody in the building can be trusted with dangerous drugs and medical records. You must be in some kind of enchanted kingdom.

In Defense of the Demon Dialer

Dear 2600:

In the Summer 92 issue The Devil's Advocate reviews our Demon Dialer. Although the tone of the review was positive, the writer said the Demon Dialer lacked in not having a chassis, speaker, battery holder, or serial connector.

We found that phone phreaks from all over the world prefer to use the speaker that couples best to the microphones in the phones of that particular country. In fact, the best speakers can often be found in "handset vending machines" that are sometimes called phone booths.

Point is that no two phreaks that we have encountered seem to like the same speaker. As for the serial connector: the things are big, and for people that do not use the Demon together with their computer (all the features can be used from the Demon Dialer keyboard) this would have been a problem. We did not have the room on the board to put it in, and enlarging it would have made the thing too big.

Some people have built the Demon inside their home phone, others have put it in a small box. Some use AA cells to power it, others use a few coin cells and still get weeks of usage out of them. Again, what chassis and batteries to use for the Demon is a matter of personal taste. We deal with the technology and prefer to sell just that. We're not into the nifty consumer cosmetics. People can and should figure out these simple things for themselves.

Since we do not make huge profits from this product, any addition to the package would drive the price up.

By the way, we did get ahold of a load of almost free battery holders for 4 AA cells, and we'll stick one with every kit, as long as we still have them. So order now and get a free $0.50 battery holder!

For people that wish to offer: please send no checks, they are absolute hell and bloody expensive to cash here in Holland. Cash or American Express traveller's checks only.

Hack Tic
Amsterdam

Slow Learners

Dear 2600:

It has been decided that my high school is bogus. The school is suffering from a lack of a math/CS department, an underfunded art department, and a bunch of burger eating morons for administration that won't do anything about it.

Because of this, I have to take all of my math/CS courses at the local university. Well, the high school has decided not to support me (or any of the others in this situation) in my decision to do this. I must take a full high school load, which in my case means 33 semester hours. This is quite a strain.

Since the administration won't do anything, I am going to.

Some time in the near future, I plan to begin distributing flyers around town describing the non-existent departments at the HS, and how the administration is standing in the way of the few students who are actually trying to get an education.

The Ryes will encourage the school board to support the addition of a new math/CS department onto the regular school curriculum, and encourage all students and faculty to strike on a date yet to be determined. I am attempting to get an endorsement from as many celebrities in the math/CS world as I can, and yours would definitely be helpful. What do you say?

Dan

How about "as printed in 2600"? Good luck.

Data

Dear 2600:

The 312 ANAC is 270-XXXX. For 708, the ANAC is hidden somewhere in the 1-200-XXXX exchange. They change it every three months, but you also find a variety of interesting things while scanning. 1-800-669-6122 ANI readout is also currently working.

Also, I have just dug up the Books of Bioc once again and found that many of the Bell News Lines still are in working order. They often hold interesting and informative tidbits on various aspects of Telecommunications. The Chicago area number is 312-368-8000.

Also, I would encourage everyone to try to start up, if not attend, a 2600 meeting. Meeting people online only goes so far.

Sarlo
Chicago

That 800 number is most interesting. When you call it the first time it thanks you for calling their 900 service and then says you've been approved for $100 worth of phone service. Then they tell you your phone number. On subsequent calls they only tell you your phone number without mentioning the 900 service. It may be nothing but this one's perked our interest. If 800 calls are being turned into 900 calls, this is one hell of a scam. Stay tuned.

Dear 2600:

Here are the ANACs for those in GTD-5 or DMS-100. (General Telephone's two most prominent switching systems.) For GTD-5 the ANAC is 1223, and for DMS-100 the ANAC is 147. These work in Southern California, and I was curious if they work in any other areas.

Those of you who are looking to practice techniques or gain more experience in voice mail hacking, try calling your local university. Most of the Cal State Universities have voice mail along with default passwords.

Tremolo

Dear 2600:

The ANAC for (701) is 490. Ringback is 410. 590 is a (1234567890) test and ANAC. What does ANAC stand for? I'm assuming it's what you dial to get the telephone's phone number. 416 cuts power to the line for about 2 minutes. 418 plus any three give you a terrible loud high pitch and so does 419 plus any three. Just wanted to give you all of what I have tried.

I picked up 2600 at a well stocked bookstore. I really like it.

Happy Reader and Reporter

Dear 2600:

Here is an ANAC that works for area code 504: 99-88-22-3303. Here is an ANAC that used to work in area code 504: 210-288-1111.

MA
Baton Rouge, LA

Dear 2600:

Read the latest issue of 2600 (which I bought at a book store here in Canada) and saw some interesting phone numbers in it. Some of them do very interesting things!

Here are some things that I have found: 1-904-321-0000 gets you a tone of some sort. It would seem that 321 is a new exchange in Tallahassee.

Also, I noticed in your Summer 1992 issue that you mentioned the 011-44-81-986-3611 number, and how it was changed to 011-44-9-10001000. I tried 011-44-9-20002000 and got a continuous tone. You might want to check it out and see what it is.

Digital Bear

The first number is a 1004 Hz tone which is a standard test tone.

Dear 2600:

The summer issue of 2600 arrived over here just a few days ago. I started reading it today. In "Fun Things To Know" on page 20 you mention the number of London information +44.81.986.3611. Well, no real news about it; I just thought you might want to know how it handles from Germany.

I've just called there and seem to get the same result as you: an intercept telling me the number has been changed to +44.9.1000.1000.

Okay, now let's dial that one.... +44.9.1000.10 (sic!) and I get an unusual German intercept along the line of "please call directory assistance". This is funny. On the first number they ask you to dial the second one including the U.K.'s country code of 44 so it is intended for foreign callers. However, the second number can't be reached.

Unfortunately I can't say whether the call is blocked in Germany or the U.K., as all erroneous calls to England generally get me a German intercept (with the exception of special announcements like a number having changed).

Naddy
Germany

Dear 2600:

The 9901 thing works in Brooklyn too. It usually says, "You have reached the (location) validation recording for the (XXX) prefix... running on a 5ESS or DMS100, etc."

Here's a cute one: dial 516-727-9858 and there's a recording that says the number has been changed to 516-727-9858. The same number! I called the operator and asked her to put the call through for me just to make her laugh.

All of the following have been tested from the 516-727 area:

9932 and 9915 give a test tone and dead line. 9911 gives a reorder signal. 9941, 9946, 9930, and 9916 all seem to be continuously busy. 9916 is odd because dialing *66 (auto redial) gives the recording "The number you are trying to reach cannot be obtained by this method."

9840, 9843, 9870, and 9871 are also always busy numbers (useful when somebody wants your number and you don't want them to call you, but you need to give them a number anyway to get them off your back).

That's about all for now. Scan your XXX-99XX, 98XX, 00XX, and 01XX exchanges today!

Sybil

We found that most of the 98XX numbers weren't busy. It's possible there are payphones that are busy most of the time. In any event, we find that most interesting numbers reside in 99XX and 00XX.

Scanner Observations

Dear 2600:

Thought I'd pass on this telecommunications tidbit.

For years I've owned a scanner and enjoy the hobby of monitoring. Way back B.C. (Before Cellular) I monitored car phones that went out over the VHF frequencies of 152.510, 152.540, 152.570, 152.600, 152.630, 152.660, ... 152.810 MHz. These phones use high power repeaters to cover the greater Los Angeles area, making it much easier to monitor an entire phone conversation and enabling me to pick up conversations in Orange County when the car is in the San Fernando valley (50 miles away).

Anyway, when the channel is not in use, I notice several states it enters. One is a fast busy (line reorder), another is the station's ID broadcast in morse code every half hour, another is some sort of automated line tester that always dials a number that is no longer in service (this is not a human being dialing, I swear), and the final mode is putting a 2600 Hz tone on the channel. I've heard the 2600 Hz tone for years, but to me it meant nothing more than some tone that my cats hate to hear and meow at incessantly until I skip to another frequency. It wasn't until I started getting into phreaking that it hit me that this was what it was. I was using a frequency generator and a primitive oscilloscope to generate a 2600 Hz tone, and as I dialed in to the correct frequency, it hit me that I've been hearing that for years.

Also significant is the fact that 2600 Hz switches are still around in North America, though it's difficult to get access to this one without a mobile phone. These phones and this switch are still in use today, though I notice the traffic is down quite a bit from what it was in the early eighties, and the drug dealers have abandoned it entirely (used to hear the most interesting conversations as their lookouts would dial number after number while sitting very bored in their cars). I enjoy your mag and look forward to the next issue.

Anon.

Where is TAP?

Dear 2600:

I have ordered two subscriptions to TAP from the address in your Marketplace section. I have not received a single issue. Do you know if they are still in business or if the address has changed or what?

IRC
Torrance, CA

While TAP was around (again) for a time, it now appears they no longer exist. So, unless you're ordering back issues from a third party, it's not a good idea to invest in TAP. We'll let you know if this changes.

Book References

Dear 2600:

I would like to understand your magazine better. Could you recommend several books for a technologically literate person to read to get up to speed on the telecommunications systems used today? The "hitchhiker's guide" in the Summer 1992 issue didn't seem to go far enough for me.

WT
Santa Barbara, CA

One that our experts agree on is Telecommunications System Engineering by Roger L. Freeman, published by Wiley Interscience. Also, try your local university library and look under telecommunications.

VMS Fun

Dear 2600:

The recent letter about auditing features of VAX/VMS systems reminded me about some of those other VMS tricks.

In your own directory, do a $ MC AUTHORIZE. AUTHORIZE is the central utility to set up accounts and rights to directories. When it doesn't find the "real" database in your directory, it'll ask if you want to create it. Sure, it won't matter. Now you have a SYSUAF.DAT in your directory which most system managers will panic over.

In V4 systems you can easily write a program using the library routines which will scan SYS$SYSTEM:SYSUAF.DAT for all accounts on the system, and specific information about them. Passwords are more difficult. But I've seen an assembly program which decoded them (ostensibly to check "weak" passwords). The first program would probably run on a V5 system. But the second wouldn't.

Allen Harker

Answering Machine Hacking

Dear 2600:

Any answering machine requiring a two digit security code is extremely easy to get into. You could try all 100 possible combinations by hand or program this number sequence into your handy Radio Shack tone dialer:

0112233445566778899135790246805

92531471593704648382726260517395
06284085296300741575316642058765
43210

Program the first 32 numbers into P1, the next 32 into P2, and so on. The five numbers left over can be stored anywhere else.

Simply call a number with an answering machine and press all "priority" keys. If the answering machine is in fact one that uses a two digit access code then you are as good as in. If you do get in there are a number of things you can do. My favorite is to press 5 on most systems and listen in on the room with the room monitor. Experiment and see what you can do.

Here are a few numbers for the 213 area code (Los Angeles):

935-1111: sweep;

Any prefix with an 0002 suffix is a phone company test line with 1004 hz tone;

111: in some areas of Los Angeles this will get you the proctor test set;

114: ANAC.

Some other numbers:

(512) 472-9941: insert 25 cents;

(512) 472-4263: WATS recording;

800-325-4112: Easylink;

800-828-6321: Xerox;

(714) 776-4511: TRW;

(714) 636-3492: TRW.

SPaDe
Montebello, CA

Of course just entering 100 codes wouldn't be too difficult. But your method definitely makes it much quicker.

A Request

Dear 2600:

Please publish all prefixes for 800 numbers. If you cannot do that how about those that work west of the Mississippi, or at least in California and Colorado.

The Har
Denver

Some years ago that would have been possible. Now, 800 exchanges are not location specific and, within a couple of months, they won't even be carrier specific. While 800-555-5000 might be using AT&T, 800-555-5001 could be using Sprint. It will be up to the customer to choose the long distance carrier of their 800 number.

Bellcore Threats

Dear 2600:

A bit of geographical irony relating to the recent attacks by Bellcore. In reading Mr. Suchyta's letter, I noticed the address. Coincidentally, I had bought that issue at the new local huge Barnes and Noble's on Route Ten, a road which becomes Mt. Pleasant Avenue. I wonder if Mr. Suchyta, writing from the "Livingston Corporate Center of Bell Communications Research" realized the increasing availability of your magazine in his immediate area. Also, no longer will I have to make the trek to St. Mark's Bookshop to get my copy. (Maybe I should subscribe!)

Valis (R&T)
West Orange, NJ

Turn to page 47 for some good reasons to subscribe.

Turn to page 47

Caller ID Hoodwinking

Dear 2600:

I just received my first issue of 2600 (the Summer 1992 issue) and read it with great interest from cover to cover. I paid particular attention to the respectively large section devoted to defeating *69 (Call Return), Caller ID, and ANI because I am/was an intervener or party of record in last year's New York State Caller ID proceeding.

I'll never forget how Arthur Miller, a top legal gun from Harvard who's always giving legal interpretations on morning television, strutted in for New York Telephone and proceeded to sway the commission to permit Caller ID and take away a huge chunk of all New Yorkers' privacy.

The New York Department of Law and the New York State Consumer Protection Agency with all their fine lawyers and arguments never had a chance against New York Tel and ol' Artie.

My interest stems from my being a reseller of services tariffed by the commission to provide toll bypass and interactive voice services (IVR). I testified that Caller ID is going to hurt my business down the road.

I program micros to be real, real smart call diverters and extenders. One of the things that wasn't really mentioned in the section on how to defeat *69 and Caller ID is that 3-way calling connections, call forwarding, and Centrex transfers *do not* transfer or pass ANI and Calling Party Name ID of the "original" caller. In effect a bogus "real" phone number is passed through these kinds of connections to Caller ID recognition devices.

Through my interrogatories or official questions I put to New York Tel and Rochester Telephone respectively, I got them to "fess up that what I just mentioned is indeed the case with their networks. It's etched in public record in between the mounds and mounds of other interveners.

So where I hope to be making lots and lots of 3-way calling connections, Centrex transfers, and employing the use of call forwarding in various applications, virtually all my applications will *inherently* defeat *69 from an entirely separate application - separating local exchange carriers from their intraLATA toll revenue above board and legal, certified by the New York State and soon Pennsylvania Public Service Commissions by tariff. It's what's known as a "Leaky PBX".

The solutions to beat *69 and Caller ID in *2600* were good but on the whole they were relatively expensive. Such methods as using calling cards, cellular phones, and operator assisted calls cost big telephone bucks to play phone hide and seek. New methods should be promoted.

With a big hunt group of, say, 100 or more "Leaky PBX" lines, a wonderfully secure environment for people who want to hide from *69 and Caller ID is an inherent attraction. With 100 incoming trunks each having the capacity to make 240 Centrex connections per hour, it doesn't take a rocket scientist to figure there's not going to be a way to determine which outgoing call from the Centrex group matches which incoming call to the lead hunt group phone number.

Sure, the answering party with Call Return or Caller ID gets the phone number of one of the Centrex group's phone numbers. So what?! While I have not yet pursued the toll bypass process on a large scale yet in New York or Pennsylvania, I just wanted to mention the option of using 3-way calling and Centrex from the local telco in conjunction with some kind of call diverter or extender as a way to beat *69 and Caller ID. I hope I have related some useful information to all who have privacy concerns.

Gabriel

Hardware Lock Info Needed

Dear 2600:

I have been searching over a year now for any information on defeating those cryptic parallel port hardware locks that specialized software companies use to keep end users from adding additional terminals to a network. I own and maintain a small network (DOS/Novell) in which I use a specialized program to run the Point of Sale touch screen cash registers for my restaurant (written in C). Each station must have one of these plugs attached to the parallel port or the station crashes. The plug itself is simply a chip (probably a serialized E Prom) on a small circuit board covered with what appears to be an epoxy type compound, making it impossible to read or remove. The only information I found was when I phoned one of the companies who make these "plugs" posing as a software producer. All I learned was how great they work, how impossible to defeat (which piqued my interest even more), and how I shouldn't even consider marketing my software without this protection. If you or any of your readers know anything about these "plugs" I would be forever in your debt.

The Pizza Maker Hacker

The word is out.

Japanese Phone Tricks

Dear 2600:

I'm a Japanese student and new subscriber to 2600. Yesterday, I got a bunch of back issues and enjoyed every page. Yours is one of the greatest publications I've ever read.

I'm a 4th grade student, so I had to find a job, and I got it! From next April, I'll work for Institute of Research (one of five large thinktanks in Japan) as a researcher. Maybe I can play with some supercomputers and other interesting technologies.

In Japan, there are some public phone phreakers. About ten years ago, NTT (Nippon Telephone and Telegram) introduced telephone cards and new public phones which had the capability of using these new cards. Before this, we had only "coin-op" ones which accepted 10 yen and 100 yen coins. The cards were magnetic and prepaid. There were four types: 500 yen, 1000 yen, 3000 yen (with novelty of 20 units), and 5000 yen (with novelty of 40 units). NTT charges 10 yen for a local three minute call (long distance calls cost more). This is considered a unit. If you have a 3000 card, you can use 320 units; a 5000 card can use 540 units.

Our telephone cards were easily modified by using some magnetic card readers/writers. Some people tried to steal public phones so that they could inspect the structure of them. And some people got arrested. Then many phreakers, poor foreign workers (they used illegal and cheap cards to make phone calls to their home countries), and yakuzas (Japanese mafias) made modifications so that these cards were usable forever (by writing infinite units onto the cards).

About a year ago, NTT decided to stop producing expensive cards (3000 and 5000) due to widespread modified cards and modification methods of the card. Now we have two types only.

Japanese Subscriber

We wonder if the modified cards still work and, if so, will they work forever? That's an interesting concept.

We suspect your definition of fourth grade differs from ours. In fact, we sure hope it does.

Assorted Info

Dear 2600:

Just finished ordering a DTMF decoder, model TDD-8, from a company called MoTron Electronics, 310 Garfield St. #4, Eugene, OR 97402, 800-338-9058 or (503) 687-2118. Their decoder, stock, comes assembled and burned in for 24 hours, but without a case. For $10 more, you get a plastic case with a red filter on the front (for the LED display) to mount it in. The stock decoder has an eight character display and 32 character memory that you can scroll through. For an additional $25 you can get a 96 character memory. It runs on 12VDC, 200mA. It has ports on it for power, audio in, and serial out (to a PC, for example). The display directly reads 0..9, and "A" for A, "b" for B, "C" for C, and "d" for D. The pound key and star key are a little different. The pound key displays as a "S" but without the vertical bars (IBM character 240 decimal looks similar), and the star key displays, as best as I can describe it, like a square box that has been separated to the upper right and lower left corners of an LED display.

The interesting thing they told me is that they are just coming out with a new version for PI's and law enforcement officials. This new edition is enclosed in a metal case, uses an LCD display instead of LED, and runs off a 9V battery. It has built-in audio isolation

from a DC power line, so you can use two alligator clips to hook onto a phone line without going through a line isolator, as you would have to for the above TDD 8 decoder. This deluxe model goes for $229 without ASCII interface and $299 with.

Anyway, I'll write further when I receive it and test it out how it performs.

Regarding Simplex locks, a company I know uses the Simplex 1000 series quite a bit, but only for the use described in the Dell manual, as a "secondary lock during working hours". The interesting thing is that all the locks had a four digit metal property tag stuck to them with double-sided tape. For some reason, I only saw digits 1-5 on the property tags, and no digit repeated. I also knew that the combinations of the locks were always some 4 digit combination of the property ID numbers, all pressed one at a time as opposed to two buttons pressed simultaneously. How's that for cutting down the number of possible combinations? Knowing this, one had only 47 combinations, or 24 possible combinations to try. Now, for the locks I did know the combinations to, the number of possible combinations were reduced by the fact that the person choosing the combination to be set liked to digit shift the property number, rolling over the digit that was shifted off the left side over to the right side of the number, and set the combination to that number. In computer science terms, this is called Rotate Left (or Rotate Right). An example is if the property number was 1234, the possible combinations were: 2341, 3412, 4123, 1234 (not likely, but possible).

Well, how's that for security? After a vacation, I forget the combo to one of these, but of course I had memorized the system they used, so I got in on the third try. Can you believe it, only three combos, and I'm still unlucky enough to get it on the third try!

Scott

Buena Park, CA

2600 Meeting Adventures

Dear 2600:

The [September] DC 2600 meeting wrapped up a couple of days ago. I thought I would share a little visit we had from the Secret Service! We can *not* confirm that it was the SS, but all evidence tends to that conclusion.

It started with some guys in sports jackets who kept walking by and sitting near us. Then, toward the end of the evening, a couple of guys in dark blue-collared t-shirts sat near us and seemed to look at us with a lot of attention. Then they proceeded to move on. A little later the same two were spotted on the level above us. Two more joined in, all dressed basically the same (dark blue-collared t-shirts). Boy, did they stick out like sore thumbs! We would occasionally stare directly at them, wave, etc. At one point we all stared at them! A couple of us got adventurous and moved to their level and closed in. One of us started chatting and he noticed "Secret Service" in small letters on one of their shirts. Then one of the guys asked if we knew anything about boxes that made beeps to perform calls. The steering group said something like "What's a box? Beeps?" Then everyone at the meeting (who was still around) decided to relocate right next to the SS guys. After noticing the 5 to 1 against odds, they deduced that it was better to move on, which they did, and that was the last we saw of them!

Techno Caster

Answers

Dear 2600:

This is in response to a letter appearing in the Spring 1992 issue by Henry H. Lightcap concerning CB-to-telephone patches and 300 baud data communication.

While it is indeed legal to have a CB station serve in the capacity of a telephone patch, FCC regulations strictly stipulate that the patch must not be automated. According to their rules, the CB station serving as the patch must be operated by a person physically at that station. That person is responsible for establishing the telephone connection and operating the transmit/receive switch for the duration of the call. That person must make sure that the person on the telephone observes FCC CB rules and must also make sure that the patch device is switched off when the call is terminated.

While licensed amateur radio operators do enjoy the luxury of automated telephone patches (or "autopatch" activated with various tones as Mr. Lightcap suggested), "lowly" Citizen's Band users must employ the services of a third party to place their calls. However, I am certain that some clever person could design a device that, to an outside listener, might sound like a person establishing a call for a CB operator (by using tones, digitized speech, etc).

I, too, have also experienced 300 baud discrimination. I can understand why some sysops might feel their line was being "tied up" at 300 baud, but if any rational thinker gives the matter a bit of thought, he/she will see that the argument is a silly one.

Most sysops allot their users a certain amount of time per day. For example, a common time limit is 60 minutes. If one user logs in at 9600 baud and remains online for 60 minutes, then he/she is also "tying up" the line just as much as a 300 baud user online for 60 minutes. What's the dilemma? Why have time limits if they are not to be respected?

Scott R.

Huntsville, AL

Address letters to:
2600 Letters
PO Box 99
Middle Island, NY 11953
or internet address
2600@wellsf.ca.us

a blast from the past

Many years ago, blue boxes were one of the phone company's biggest concerns. Here is how one branch of the old Bell System educated its employees:

Electronic Toll Fraud Devices

There are several different types of electronic equipment which may be generally classified as ETF devices. The most significant is the "blue box". The characteristics of each type of device are discussed below.

Blue Box

The "blue box" was so named because of the color of the first one found. The design and hardware used in the blue box is fairly sophisticated, and its size varies from a large piece of apparatus to a miniaturized unit that is approximately the size of a "king-size" package of cigarettes.

The blue box contains 12 or 13 buttons or switches that emit multifrequency tones characteristic of the tones used in the normal operation of the telephone toll (long-distance) switching network. The blue box enables its user to originate fraudulent ("free") toll calls by circumventing toll billing equipment. The blue box may be directly connected to a telephone line, or it may be acoustically coupled to a telephone handset by placing the blue box's speaker next to the transmitter of the telephone handset. The operation of a blue box will be discussed in more detail below.

To understand the nature of a fraudulent blue box call, it is necessary to understand the basic operation of the Direct Distance Dialing (DDD) telephone network. When a DDD call is properly originated, the calling number is identified as an integral part of establishing the connection. This may be done either automatically or, in some cases, by an operator asking the calling party for his telephone number. This information is entered on a tape in the Automatic Message Accounting (AMA) office. This tape also contains the number assigned to the trunk line over which the call is to be sent. The assigned trunk number provides a continuity of information contained on the tape. Other information relating to the call contained on the tape includes: called number identification, time of origination of call, and information that the called number answered the call. The time of disconnect at the end of the call is also recorded.

Although the tape contains information with respect to many different calls, the various data entries with respect to a single call are eventually correlated to provide billing information for use by Southern Bell's accounting department. The typical blue box user usually dials a number that will route the call into the telephone network without charge. For example, the user will very often call a well-known INWATS (toll-free) customer's number. The blue box user, after gaining this access to the network and, in effect, "seizing" control and complete dominion over the line, operates a key on the blue box which emits a 2600 Hertz (cycles per second, abbreviated hereafter as "Hz") tone. This tone causes the switching equipment to release the connection to the INWATS customer's line. Normally, the 2600 Hz tone is a signal that the calling party has hung up. The blue box simulates this condition. However, in fact the local trunk on the calling party's end is still connected to the toll network. The blue box user now operates the "KP" (key pulse) key on the blue box to notify the toll switching equipment that switching signals are about to be emitted. The user then pushes the "number" buttons on the blue box corresponding to the telephone number being called. After doing so, he operates the "ST" (start) key to indicate to the switching equipment that signalling is complete. If the call is completed, only the portion of the original call prior to the emission of 2600 Hz tone is recorded on the AMA tape. The tones

THE INVESTIGATION AND PROSECUTION OF ELECTRONIC TOLL FRAUD CASES

FOR OFFICIAL USE ONLY

Southern Bell

emitted by the blue box are not recorded on the AMA tape. Therefore, because the original call to the INWATS number is toll-free, no billing is rendered in connection with the call.

Although the above is a description of a typical blue box operation using a common method of entry into the network, the operation of a blue box may vary in any one or all of the following respects:

(a) The blue box may include a rotary dial to apply the 2600 Hz tone and the switching signals. This type of blue box is called a "dial pulser" or "rotary SF" blue box.

(b) Entrance into the DDD toll network may be effected by a pretext call to any other toll-free number such as Universal Directory Assistance (555-1212) or any number in the INWATS network, either inter-state or intra-state, working or non-working.

(c) Entrance into the DDD toll network may also be in the form of "short haul" calling. A "short haul" call is a call to any number which will result in a lesser amount of toll charges than the charges for the call to be completed by the blue box. For example, a call to Birmingham from Atlanta may cost $.60 for the first three minutes while a call from Atlanta to Los Angeles is $1.65 for three minutes. Thus, a short haul, three-minute call to Birmingham from Atlanta, switched by use of a blue box to Los Angeles, would result in a net fraud of $1.05 for a three-minute call.

(d) A blue box may be wired into the telephone line or acoustically coupled by placing the speaker of the blue box near the transmitter of the telephone handset. The blue box may even be built inside a regular Touch-Tone (r) telephone, using the telephone's pushbuttons for the blue box's signalling tones.

(e) A magnetic tape recording may be used to record the blue box tones representative of specific telephone numbers. Such tape recordings could be used in lieu of a blue box to fraudulently place calls to the telephone numbers recorded on the magnetic tape.

All blue boxes, except "dial pulser" or "rotary SF" blue boxes, must have the following four common operating capabilities:

(a) It must have signalling capability in the form of a 2600 Hz tone. This tone is used by the toll network to indicate, either by its presence or its absence, an "on-hook" (idle) or "off-hook" (busy) condition of the trunk.

(b) The blue box must have a "KP" key or button. "KP" is an abbreviation for a "Key Pulse" tone that unlocks or readies the multi-frequency receiver at the called end to receive the tones corresponding to the called telephone number.

(c) The typical blue box must be able to emit multi-frequency tones which are used to transmit telephone numbers over the toll network. Each digit of a telephone number is represented by a combination of two tones. For example, the digit 2 is transmitted by a combination of 700 Hz and 1100 Hz tones.

(d) The blue box must have an "ST" key. "ST" is an abbreviation for a "start" signal which consists of a combination of two tones that tell the equipment at the called end that all digits have been sent and that the equipment should start switching the call to the called number.

The "dial pulser" or "rotary SF" blue box requires only a dial with a signalling capability to produce a 2600 Hz tone.

IS AT&T HIDING NEAR YOU?

[illegible]

CONNECTICUT

[illegible]

DELAWARE

[illegible]

DISTRICT OF COLUMBIA

[illegible]

MAINE

[illegible]

MARYLAND

[illegible]

MASSACHUSETTS

[illegible]

NEW HAMPSHIRE

[illegible]

NEW JERSEY

[illegible]

NYNEX

[redacted]
BROOKLYN NY

October 22 1992

Payment Due: October 21, 1992
Ac [redacted]
Amt: $[redacted]

Dear [redacted]

I had hoped to talk with you about this month's unusually high bill, but I was unable to reach you by telephone.

I know that this bill in itself is not necessarily a matter of great concern. It has been my experience - with personal and on the job - that a bill so much higher than usual, whether expected or not, often seems to arrive at just the wrong time in terms of impact on the budget. I wanted to let you know - if that is the case in this instance - that we understand and, if you wish, we would be glad to discuss payment arrangements.

If you have already mailed your payment, I thank you, and there is no need to reply, of course, but if not, I would like you to discuss it with your Representative. I would appreciate your calling us on [redacted], at your earliest convenience.

Sincerely,

[redacted]
Manager

NYNEX had the nerve to send this loyal customer a semi-warning letter a full half month before the bill was even due!

2600 marketplace

2600 MEETING INFO: Turn to page 46.

WANTED: EPROM programmer / programming adapter compatible with 8Xxx series microcontrollers. Will Trade or purchase. Contact Travis at (916) 754-2063.

COMPUTER VIRUS DEVELOPMENTS QUARTERLY is the totally radical new quarterly journal covering the whole field of viruses, dedicated to making this info public knowledge. Each issue includes a disk. This winter's features: source code infection and the Virus Creation Lab. Send $75 for a year's subscription, or send $10 for a sample issue (no disk). American Eagle Publications, Box 41401, Tucson, AZ 85717.

LOOKING FOR HELP. Any and all information, plans, books, schematics, etc. relating to hacking, phreaking, electronics, computers, phones, cable tv. Will share research info with all. Also, I need the address to Radio Electronics magazine and Popular Electronics magazine. Contact Salvatore Grasso #235125, M.S.C.F., P.O. Box 866, Wrightstown, NJ 08562.

6TH INTERNATIONAL COMPUTER SECURITY & VIRUS CONFERENCE at Manhattan Ramada (by Penn Station). 5 tracks, 90 speakers, 70 vendors, $395. 3/10/93-3/12/93 (Wednesday-Friday). Heavy emphasis on viruses and telecom fraud. Special sessions on LAN and management track. Intro to security. NEIWARE exhibit for non-attendees - fax business card to (303) 825-9151, your badge will be mailed. For registration, call 800-835-2246, extension 190.

ARRESTED DEVELOPMENT. H/P/A/V. +31.79.426079. Renegade 8-10 UUCP DOMAINS: Vinnet Node, PGP Areas, 386-33mhz, 300mb, USR DS 38k4.

LOOKING FOR ANYONE and everyone wanting to trade ideas, Amiga files, info about "interesting" things. I have about 10 megs of text files, ALWAYS looking for more! Contact Steve at 414-422-1067 or email dipper@csd4.csd.uwm.edu

WE CAME, WE SAW, WE CONQUERED. 11" x 17" full color poster of pirate flag flying in front of AT&T facility. Send $6 to P.O. Box 771072, Wichita, KS 67277-1072.

PHONES TAPPED, office/home bugged, spouse cheating. Then this catalogue is for you! Specialized equipment, items, and sources. It's time to get even. Surveillance, countermeasures, espionage, personal protection. Send $5 check or money order to B.B.I., PO Box 978, Dept. 2 6, Shoreham, NY 11786.

TAP BACK ISSUES. complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 661, Mt. Laurel, NJ 08054. We are the Original!

PRINT YOUR ZIP CODE IN BARCODE. A great label program that allows you to use a database of address to print label with barcode. You also type and print a custom label. Send $9 no check to: H. Kindel, 5662 Calle Real Suite 171, Goleta, CA 93117. IBM only.

GENUINE 6.5536 MHZ CRYSTALS only $5.00 each. Orders shipped postpaid via First Class Mail. Send payment with name and address to Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083. Also information wanted on Northeast Electronics Corp's TTS-59A portable MF sender and TTS-276GR MF and loop signalling display. Need manuals, schematics, alignment and calibration instructions (or photocopies). Will reward finder.

WIRELESS MICROPHONE and wireless telephone transmitter kits. Featured in the WINTER 1991-92 2600. Complete kit of parts with PC board, $20 CASH ONLY, or $35 for both (no checks). DEMON DIALER KIT as reviewed in this issue of 2600. Designed and developed in Holland. Produces ALL voiceband signals used in worldwide telecommunications networks. Send $250 CASH ONLY (DM 550) to Hack-Tic Technologies, Postbus 22953, 1100 DL Amsterdam, Netherlands (allow up to 12 weeks for delivery). Please call +31 20 6001420 / 1441. Absolutely no checks accepted!

FORMER U.S. ARMY ELECTRONIC WARFARE TECHNICIAN with TS clearance looking for surveillance work which requires cunning, ingenuity, and skill. Protocks of Atlantic City, Box 1769, Atlantic City, NJ 08404.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Spring issue: 2/15/93.

telco news

We've seen a good deal of ineptitude on the part of phone companies over the years. But we're still capable of being surprised. SouthWestern Bell (SWBT) wins the prize in the latest round. Some numbers to their computers have been circulating for some time. Specifically, 316-261-1713, 316-261-1716, 316-261-1717, 316-261-1200, 316-261-1222, and 316-261-1229. The numbers themselves are insignificant; every phone company's computer dialups have been found by someone. It's the line of defense that exists after the computer picks up that is the true test of security. A writer we know was quite surprised when, while verifying the authenticity of one of these numbers, he accidentally got root access to the system! He had typed root as a joke thinking that would be the quickest and surest way to disconnect. Not so. He was instantly welcomed with open arms. The writer quickly hung up but this event raises some real troubling questions. Like where has SouthWestern Bell been lately? Don't they realize the importance of secure, non-obvious passwords, particularly for their most powerful account? How many people will be lured in by this seeming lack of concern? And finally, is this person now guilty of "breaking into" a phone company computer when that was never the intention?

In light of this occurrence, how can we take recent SWBT claims seriously? They seem to think that hackers are the root (no pun) of all of their problems. A recent SWBT publication claims that hackers who caused no damage cost the company lots of money. "The loss to SWBT is estimated at $870,000. That includes expenses for securing the packet network to avoid future intrusions, reprogramming costs and labor for an internal investigation."

"SWBT's efforts to prevent hackers include restructuring various communications networks and adding security hardware to computer systems.

"Employees serve as an important line of defense against hackers, said Barry Rabin, area manager-asset protection.

"'The easiest way for a hacker to get into our computer is to obtain a password through what's known as "social engineering,"' said Rabin.

"'The hacker calls an employee and pretends to be another employee who needs a password to check on a job,' Rabin said.

"'To guard against social engineering, Rabin recommends making sure you know who you're talking to.

"'It doesn't cost anything to confirm the identity of the caller by getting a number and making a call-back check,' Rabin said. 'Employees who receive any suspicious calls should contact the asset protection division or their interdepartmental security forum representative as soon as possible.'"

If you'd like more information on the practice of social engineering, SWBT's computer security administration group actually has an employee education campaign on the subject. Posters and other information for the campaign can supposedly be obtained by calling Jackie Smick at 314-235-9082.

SWBT is urging its employees to be alert. It seems pretty obvious to us that these employees just aren't doing all they can. In fact, we think they need all the help they can get. SWBT tells its employees "If you receive a suspicious phone call with a request for a company phone directory, computer password, or other proprietary information, the caller could be a computer hacker. To be safe, ask for a name and a call-back number, then contact your interdepartmental security forum representative." It might be a good idea for the rest of us to keep on the alert for those wide open security holes you could bank a truck through. If you find any, what better way to show your good intentions than by helping these poor souls out? These are the security "experts" for SWBT's various regions:

Arkansas:Don Miller:501-373-5372
Kansas:Mike Leck:316-268-3247
Missouri:Bob Fields:314-247-6022
Oklahoma:Charles Gass:405-278-4246
Texas:Renee Johnson:214-464-7907

Internal security memorandums of more than a year ago indicate that SouthWestern Bell was aware it had some major security holes. "Potentially ALL systems utilizing [the packet] network COULD HAVE BEEN COMPROMISED AND INTRUDED" was the dire warning in one memo. "Administrative controls SHOULD be placed on vendor support links, including dial-up ports and packet gateways." Whether or not anything was ever actually done, it would appear that sloppiness is once again the rule.

An internal Bellcore bulletin concerning the security of packet switched networks goes into detail on how hackers believed to be affiliated with the Legion of Doom and 8LGM hacker groups took advantage of "OA&M diagnostic software tools (e.g., XRAY from TYMNET and TDT2 from SPRINTNET)" to get into the Public Packet Switched Network (PPSN) of various phone companies.

"The intruders gained access to a vendor supported OA&M 'debug' port to the BCC's TYMNET based PPSN. By exploiting the group based or default password the intruders then executed the program known as XRAY, and its utilities, to read the

```
CONNECT 1200

crasw!
WARNING!! - THIS IS A SOUTHWESTERN BELL TELEPHONE SYSTEM, RESTRICTED TO
OFFICIAL BUSINESS. UNAUTHORIZED ACCESS, USE, OR MODIFICATION IS A VIOLATION
OF LAWS AND MAY SUBJECT THE PERPETRATOR TO CRIMINAL PROSECUTION.
login: root
Password:

Welcome!

JOTCSW + ACCS USERS: You are low on space.
Please clean up your files.

Reminder: Network meeting tomorrow at 10:00 a.m.

erase = backspace
kill = @
```

data traffic on any of the X.25 port line cards and MUX multiplexers. By reading the data of the X.25 port line cards or MUXs, and scanning the memory space internal to the packet handler, the intruders were able to capture logins and passwords transiting over or used within the packet network. With the help of the compromised logins and associated passwords, the intruders then attacked: 1) the computer systems and networks that were being addressed during the compromised packet sessions, or 2) the networked hosts to the packet handler."

The Bellcore bulletin targets a Legion of Doom/Hackers oriented bulletin board system and concludes that "the intruders have perfected their skills and have utilized that knowledge to compromise the PPSNs of several carriers. Once compromised, the intruders are able to capture data including logins and passwords from the PPSN traffic." Packet networks at risk included SPRINTNET (TELENET), TYMNET, Bell Atlantic's PDN, BellSouth's PULSELINK, Pacific Bell's PPS, Southern New England Telephone's ConnNet, and NYNEX's NYNEXLAN.

Bellcore clearly believes that hackers are nothing short of terrorists. A security alert from November 1990 warns that "the potential for security incidents this holiday weekend is significantly higher than normal because of the recent sentencing of three former Legion of Doom members. These incidents may include Social Engineering, computer intrusion, as well as possible physical intrusion." Pages are devoted to "suggested countermeasures" to counter the expected onslaught of attacks.

With this kind of paranoia running rampant in the hallowed halls of the phone companies, how is it that they still manage to leave the front door wide open?

Yellow Pages Screening

Ever wonder where the phone companies draw the line on Yellow Pages advertising? We caught a glimpse of some internal NYNEX guidelines that define unacceptable advertising.

"Advertisements which are, in the opinion of the publisher, indecent, vulgar, obscene, suggestive, or offensive, either in direct presentation or by suggestion in the text or illustration, will not be accepted under any heading.

"Particular care should be exercised in reviewing advertising copy and illustrations for placement at any of the sensitive headings listed below....

"Balloons, Book Dealers, Dating Bureaus, Entertainers, Modeling Agencies, Massage, Motels, Motion Picture Producers, Night Clubs, Telegrams, Theatres, Escort Service.

"... Objectionable copy or illustration will be refused at any heading.... What is appropriate at one heading may take an entirely different meaning at another heading. For example, a person in a swim suit may be appropriate at "Swimwear & Accessories" but may communicate an offensive message at "Escort Service - Personal".

What Isn't Acceptable

"If the advertisement as a whole implies that the firm is something other than a legitimate establishment", the advertisement won't be printed.

(continued on page 46)

PRODUCT REVIEW

Speech Thing by Convox Inc.
Suggested retail: $79.99
Available from just about any PC mail order house
Review by Cray-Z Phreaker
Special thanks to those who know...

When I received the package from the UPS man, I was mildly surprised. The box was *quite* large for the application that I had in mind for the device. Much to my relief, upon unpacking the unit, it was revealed to be much smaller... perfect for what I had in mind. But let's not get ahead of ourselves.

Convox's *Speech Thing* is an add-on audio port for IBM/clone computers. It attaches to the machine via the parallel port, and comes with a rather large external speaker (9v powered). The device itself is the same size as a common "gender changer". A pair of wires protrude from one side of the device that attach to the external speaker. Just plug it in to the back of your machine, attach the speaker, and you are ready to go! Software installation is mindless, and straightforward.

The software itself isn't difficult to use, so I won't bother going into detail about that here. Let's talk about uses for the device.

After seeing the *Hack-Tic* Demon Dialer at SummerCon, I was very interested in the device, but like many phreaks, I didn't have $250 lying around to spend on it. An alternative was needed, and since I have a cheap portable PC clone, why not utilize it somehow? Granted it's not as slick as the dialer, but I'm not worried about that right now. Upon hearing from some other phreaks (who would like to remain anonymous) about the *Speech Thing*, and their uses of it as a red box, I ordered one with the idea that it could do more... much more.

After testing out the unit with the red box sound file, I was impressed with the sound quality of the device, but not happy with the speaker itself. It's kinda large and didn't fit in my portable case well. The Radio Shack Mini Amplifier/Speaker (cat no. 277-1008C) is a good substitute, is 9v powered, and most importantly, it's small in size.

Now we have a small, programmable, portable tone generator. What more could a phreak ask for? Granted you have to have a portable computer, but most serious phreaks have one anyway. Now all we need is some useful software. I've been working on some software in my spare time, but it's far from being completed. With a telephone interface, there is no reason that this device couldn't do the same as the *Hack-Tic* dialer. If you add the sound digitizer option, your capabilities expand beyond that of the $250 dialer.

I had some difficulty with the *Speech Thing* on my Toshiba T-1000. Occasionally the playback rate changes a bit, then reverts back to the original setting while using the software supplied. When red boxing, you will get an AT&T operator online quick if you don't get in another "good" quarter. I have only seen this quirk when using the Toshiba T-1000 machine. It seems to work flawlessly with other portables.

If you have a portable and $80 available, I highly recommend this device as a basic tool for phreaking.

Enjoy and please write in with whatever experiences you have with the device.

telco news

(continued from page 44)

Phrases that aren't acceptable include those which "refer to the sex, suggest nudity, or the physical description of the business staff".

There are also certain words and phrases you cannot ever use. These include "Young Technicians", "Once is never enough", Slip and slide oil rubs", "Hot Bodies for the man who has no limits", "We take it all off to music", "Strip Tease Dancers", "We show it all", "Full Nudity", and, of course, "Full". Other words include: "Strip", "Strip-o-Grams", "Full Show", "Topless", "Fantasy", "Nude", "Stripper", "Teletease Telegrams", "1/2 Full Show", and "Bottomless". We should point out that "Nude" and "Full" are only unacceptable when they are used to imply nudity.

Finally, the pictures/illustrations deemed unacceptable include: "Male or female forms alluding to sex or that are provocative in nature. Illustrations with expressive cleavage or bare buttocks will not be permitted; [as well as illustrations] that suggest sensual or erotic pleasures; male or female forms without proper street attire; and suggestive poses".

So now you know.

2600 MEETINGS

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: 212-223-9011,8927; 212-308-8044,8162.

Washington DC

Pentagon City Mall in the food court.

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: 215-222-9880, 9881, 9779, 9799, 9632; 215-387-9751.

Chicago

Century Mall, 2828 Clark St., lower level, by the payphones: 312-929-2695, 2875, 2685, 2994, 3287.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World. Payphones: 512-453-9834, 9865, 9916.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: 213-972-9358, 9388, 9506, 9519, 9520; 213-625-9923,9924; 213-614-9849, 9872, 9918,9926.

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.